Quelques fonctionnalités au niveau 2

ARP

VLAN

STP

P. Laurençot

Rappel sur le Routage

Et

ARP

(Address Resolution Protocol)

Table de routage

- *Tout équipement de niveau 3 à une table de routage*
  - PC, routeur, mais ni HUB, ni switch

- Composition d'une table de routage
  - 4 colonnes (ou lignes):
    - **@ réseau distant**
    - **Masque du réseau distant**
    - **@IP du saut suivant pour atteindre le réseau distant**
    - **Interface de sortie**

La table de routage ne donne que l'@IP du prochain système sur la route vers la destination

(hop by hop)

Fonctionnement table de routage

- Exemple de table de routage du routeur 193.65.20.1

@IP réseau distant	Masque	@IP saut suivant	interface
193.65.20.0	255.255.255.0	193.65.20.1	eth0
136.30.0.0	255.255.0.0	193.65.20.254	eth0
0.0.0.0	0.0.0.0	193.65.20.100	eth0

- Utilisation de la table de routage
  - Soit @Ipd adresse de destination finale
  - Pour chaque ligne de la table de routage
    - faire un "et" binaire entre @Ipd et Masque
    - Comparer le résultat avec l'@IP réseau distant
      - Si différente, passer à la ligne suivante
      - Sinon @IP du prochain saut = @IP saut suivant pour le paquet
  - Si plus de ligne, échec, abandon du paquet

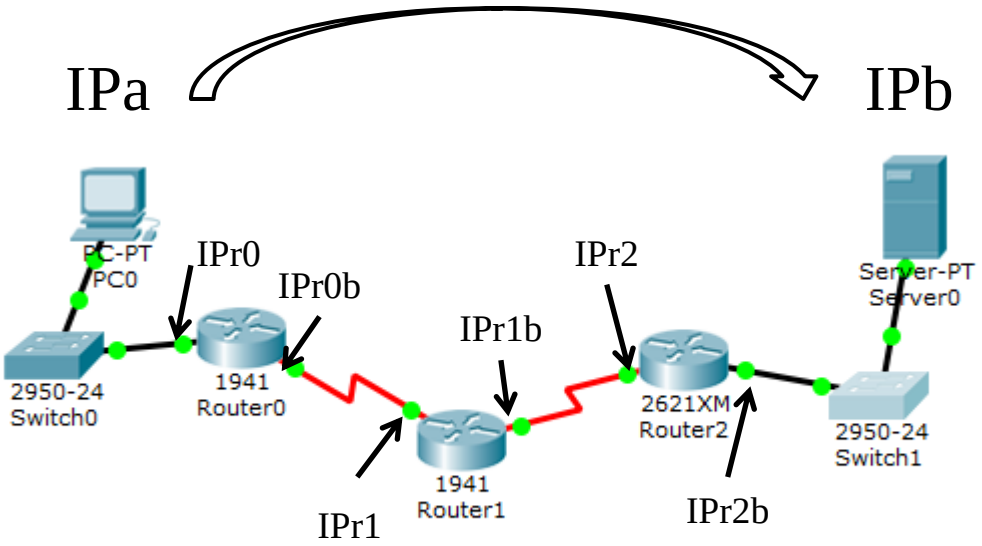
Commande pour voir la table de routage : netstat –r ou ip route

Exemple table de routage

```
IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0    172.16.79.254    172.16.65.100    276
        127.0.0.0        255.0.0.0          On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255          On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255          On-link         127.0.0.1    306
      172.16.64.0    255.255.240.0          On-link    172.16.65.100    276
    172.16.65.100  255.255.255.255          On-link    172.16.65.100    276
    172.16.79.255  255.255.255.255          On-link    172.16.65.100    276
     192.168.56.0    255.255.255.0          On-link     192.168.56.1    276
     192.168.56.1  255.255.255.255          On-link     192.168.56.1    276
   192.168.56.255  255.255.255.255          On-link     192.168.56.1    276
        224.0.0.0        240.0.0.0          On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0          On-link     192.168.56.1    276
        224.0.0.0        240.0.0.0          On-link    172.16.65.100    276
  255.255.255.255  255.255.255.255          On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255          On-link     192.168.56.1    276
  255.255.255.255  255.255.255.255          On-link    172.16.65.100    276
===========================================================================
Itinéraires persistants :
  Adresse réseau    Masque réseau  Adresse passerelle Métrique
          0.0.0.0          0.0.0.0    172.16.79.254  Par défaut
===========================================================================
```

Sous windows, lecture de bas en haut….

Utilisation routage (1)



4 réseaux - (Ipa et IPr0) (IPr0b et IPr1) - (IPr1b et IPr2) - (IPr2b et Ipb)

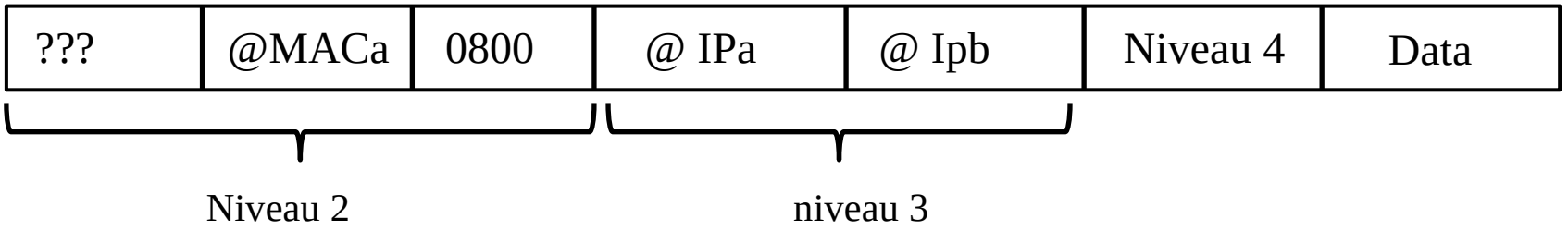
Constitution de la trame

@MACd	@MACs	type IP	@ IP source	@ IP desti	Niveau 4	Data

Niveau 2 niveau 3

Utilisation routage (2)

Constitution de la trame



- utilisation de la table de routage

Mais récupération de l'@IP du saut suivant !!!
On cherche ⟶ @MAC

ARP : Address Resolution Protocol

correspondance @MAC ⟷ @IP

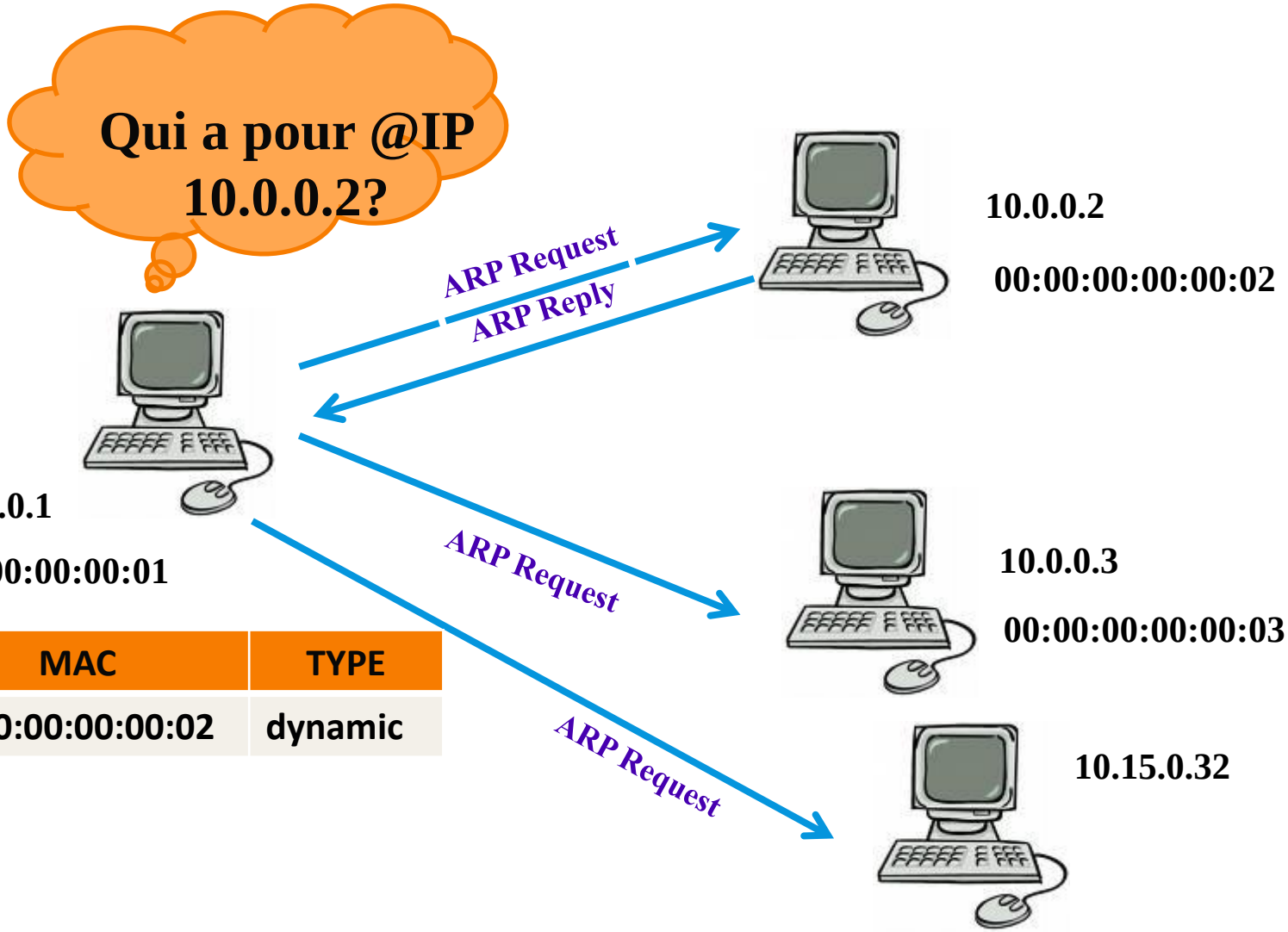
ARP (1)

ARP

- *But :* obtenir une correspondance entre @IP d'un PC et son adresse MAC

- *A* désire envoyer un message à une station *B*, et connaît son adresse IP. Mais, adresse MAC inconnue pour envoyer sa trame Ethernet.
- *A* envoie donc un *broadcast* Ethernet ARP qui contient l'adresse IP demandée (*B*) .
- Toutes les stations reçoivent ce message et examinent l'adresse IP demandée.
- Seule la station *B* répond à la requête ARP. Elle insère dans la réponse sa propre adresse MAC. Réponse en unicast.
- La station *A* récupère le message, stocke dans sa table ARP la correspondance @IP⟺ @MAC et peut maintenant envoyer des données à la station *B* en utilisant cette adresse MAC.

ARP (2)



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

ARP (3)

- 2 étapes
  - On regarde dans table ARP si correspondance (arp –a)

    (stockage temporaire des informations)
  - Une requête ARP est faite sur le réseau

No.	Time	Source	Destination	Protocol	Length	Info
111	13.464961	192.168.1.1	192.168.1.17	TCP	54	80 → 53795 [ACK] Seq=2473 Ack=4501 Win=13343 Len=0
112	13.502360	192.168.1.17	192.168.1.1	TCP	54	53796 → 80 [ACK] Seq=3746 Ack=2175 Win=254 Len=0
113	13.517112	SamsungE_be:e0:fe	Broadcast	ARP	42	Who has 192.168.1.17? Tell 192.168.1.18
114	13.517202	HonHaiPr_53:55:9b	SamsungE_be:e0:fe	ARP	42	192.168.1.17 is at 64:27:37:53:55:9b

```
> Frame 113: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: SamsungE_be:e0:fe (bc:b1:f3:be:e0:fe), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: SamsungE_be:e0:fe (bc:b1:f3:be:e0:fe)
    Sender IP address: 192.168.1.18
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.17
```

```
C:\Users\Isima>arp -a

Interface : 172.16.65.100 --- 0xb
  Adresse Internet      Adresse physique      Type
  172.16.64.4           98-e7-f4-ec-32-33     dynamique
  172.16.64.5           18-03-73-32-cb-11     dynamique
  172.16.64.9           48-4d-7e-d0-29-b6     dynamique
  172.16.64.38          b8-ca-3a-ba-2e-38     dynamique
  172.16.64.70          18-03-73-d5-39-2b     dynamique
  172.16.64.86          18-03-73-d6-6d-25     dynamique
  172.16.64.99          00-1c-c0-52-ba-af     dynamique
  172.16.64.102         18-03-73-d6-5a-75     dynamique
  172.16.64.103         18-03-73-d6-61-61     dynamique
  172.16.64.106         d4-be-d9-da-78-80     dynamique
  172.16.64.112         00-24-e8-30-33-f3     dynamique
  172.16.64.117         18-03-73-d6-5c-19     dynamique
  172.16.64.130         c8-1f-66-d1-9a-f4     dynamique
  172.16.64.133         b8-ac-6f-a2-18-44     dynamique
  172.16.64.250         e0-cb-4e-12-78-0a     dynamique
  172.16.64.252         90-e6-ba-60-50-2f     dynamique
  172.16.65.13          d4-be-d9-63-78-f7     dynamique
  172.16.65.65          d0-67-e5-3b-20-ab     dynamique
```

ARP - généralité

- ARP (Address Resolution 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 - 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*		

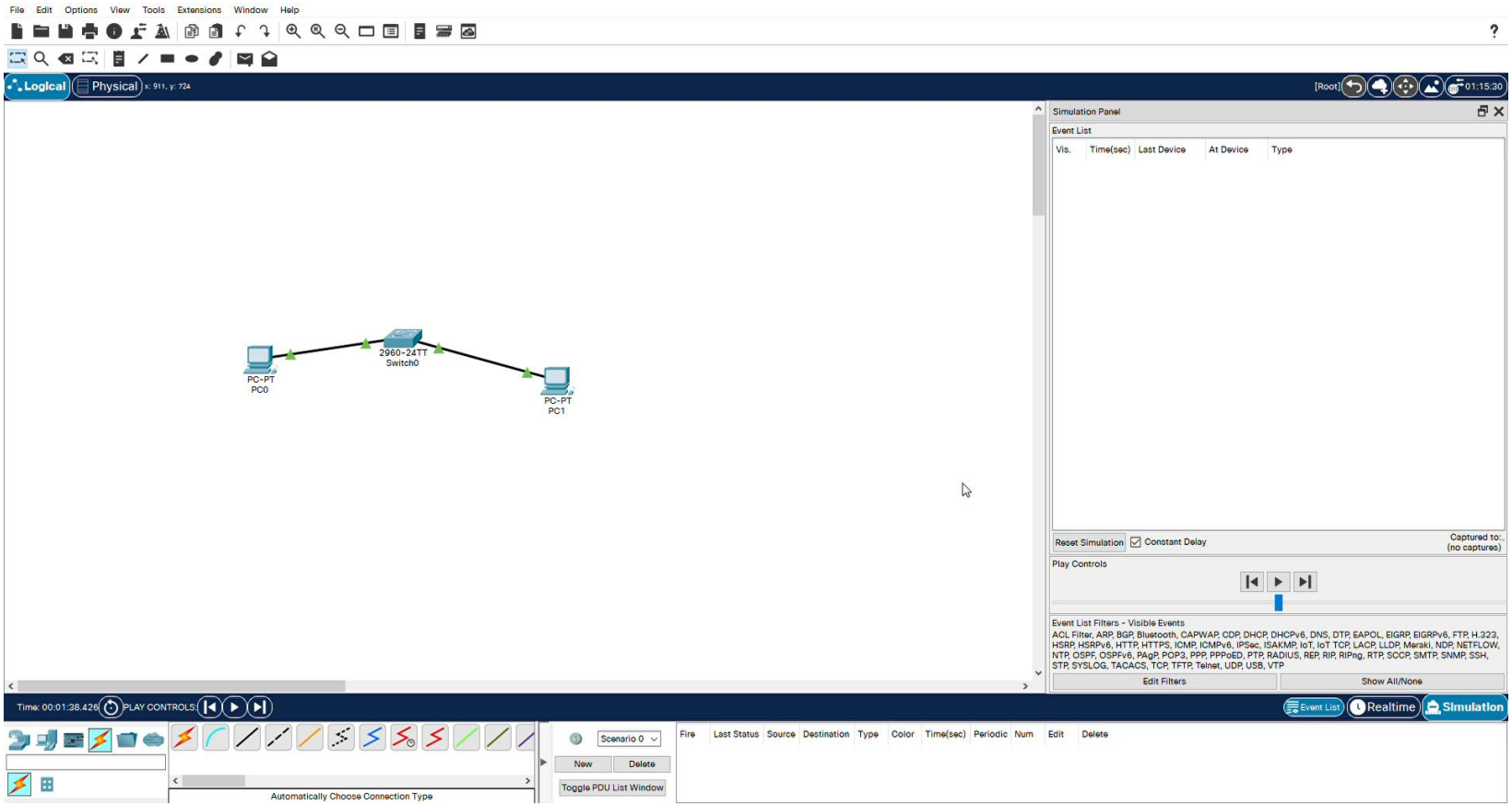
Hardware address length : 06 ethernet

Protocol Address length : 04 pour IPv4 , 16 pour Ipv6

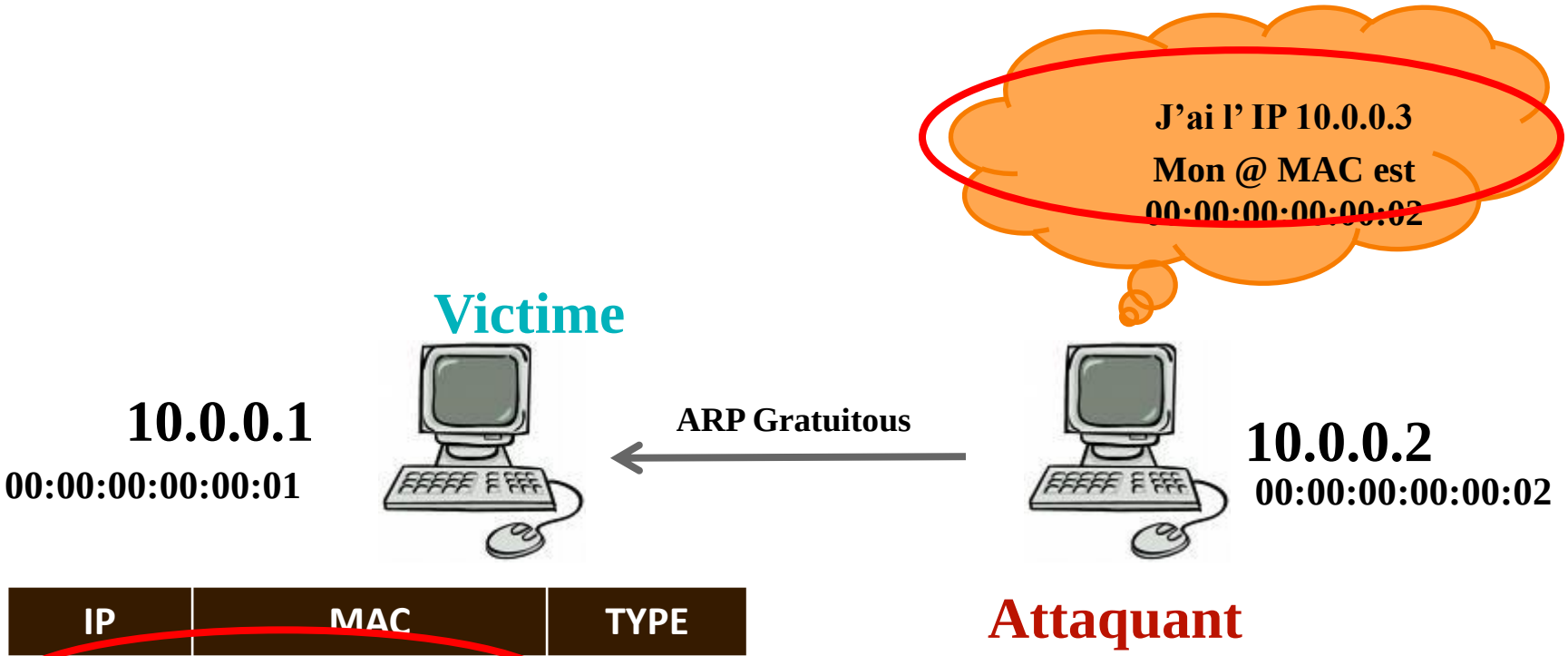
Opération : 1 requête

2 : réponse

ARP (suite)


File Edit Options View Tools Extensions Window Help
Logical
Physical
[Root]
01:15:30
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
At Device
Type
2960-24TT
Switch0
PC-PT
PC0
PC-PT
PC1
Reset Simulation
Constant Delay
Captured to:
(no captures)
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:01:38.428
PLAY CONTROLS:
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Automatically Choose Connection Type

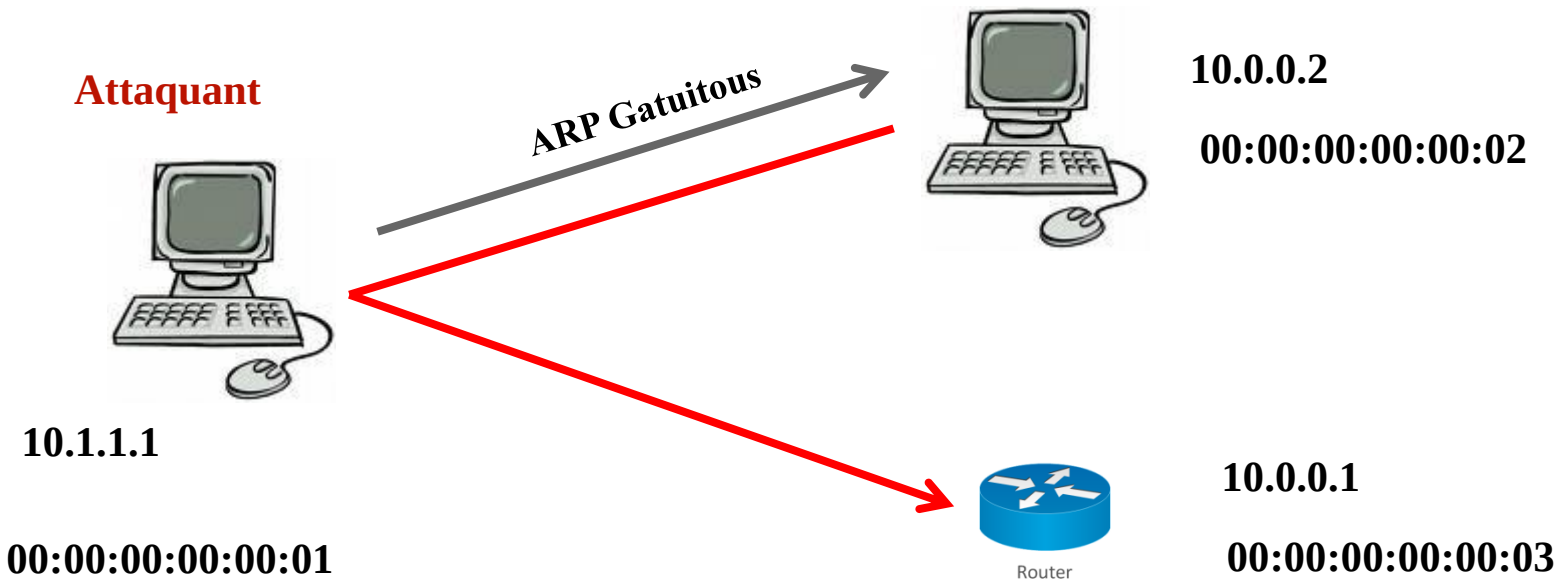
ARP spoofing (1)



IP	MAC	TYPE
10.0.0.3	00:00:00:00:00:02	dynamic

ARP spoofing (2)

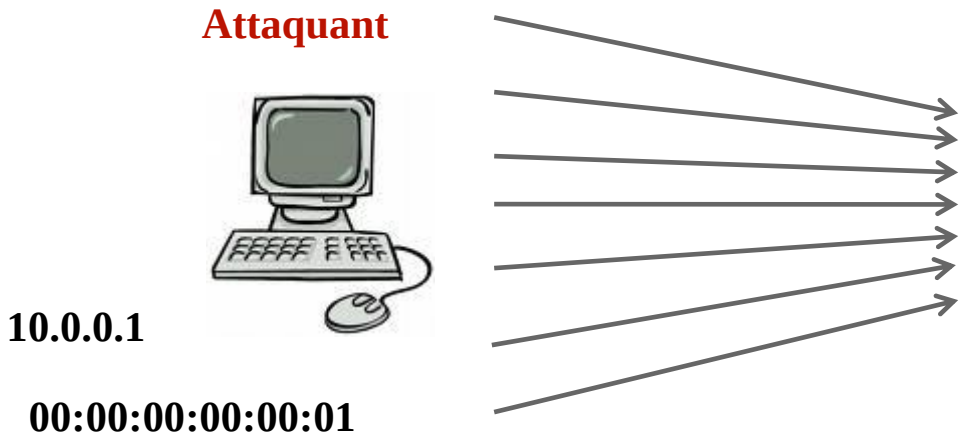
IP	MAC	TYPE
10.0.0.1	00:00:00:00:00:01	dynamic



Création de l'attaque Man in the Middle

Mac flooding

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



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 bloquer les ARP gratuitous

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

Utilisation routage (2 bis)

Attention

- La réponse à une requête ARP prend du temps

  - Pas le temps d'attendre pour certains protocoles (ICMP)

    $\Longrightarrow$ Renvoi fail à la demande

Pour le ping (ICMP)

minimum 2 essais

Windows : 5 essais
Cisco : 4 essais
Linux : infini,…