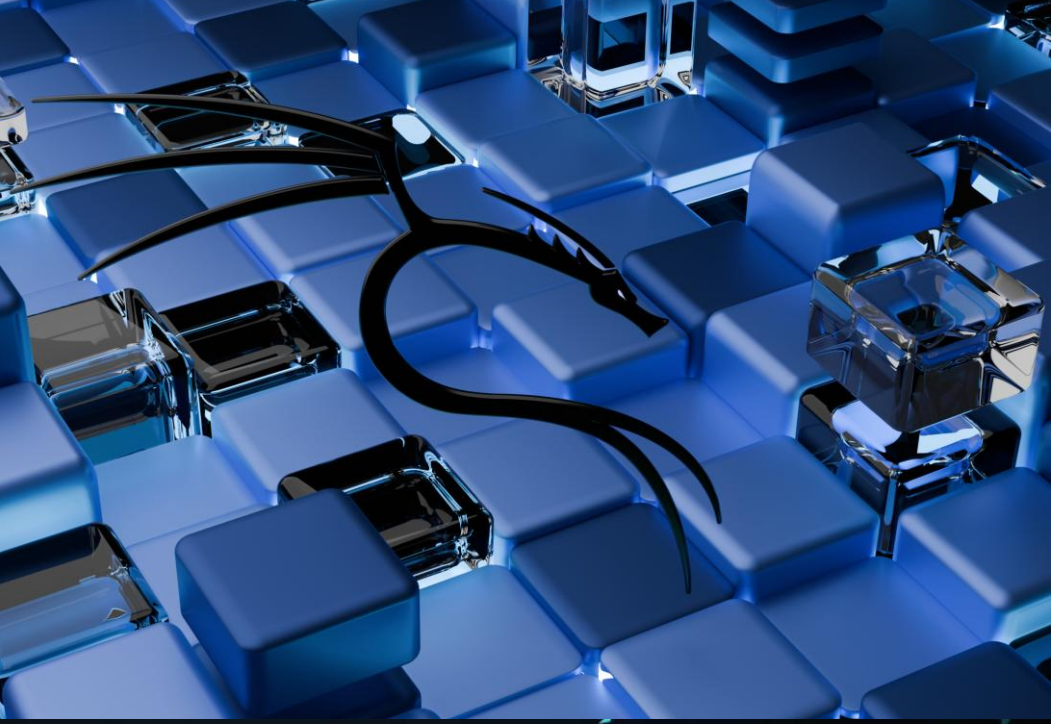
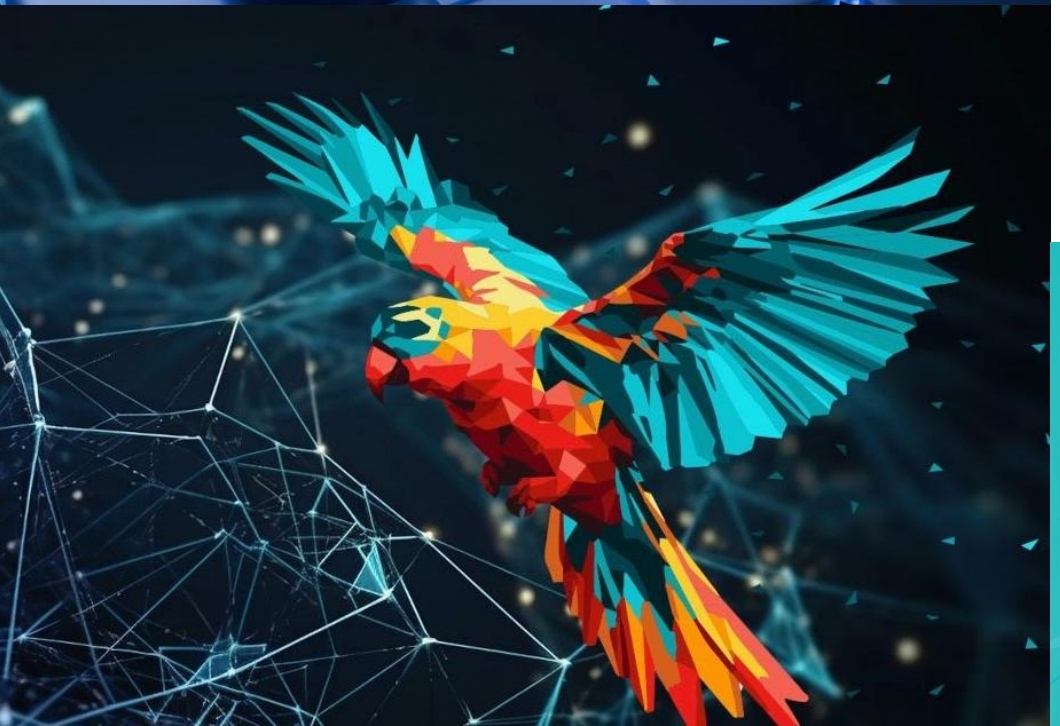




Universidad Nacional del Altiplano | Escuela Profesional de Ingeniería de Sistemas

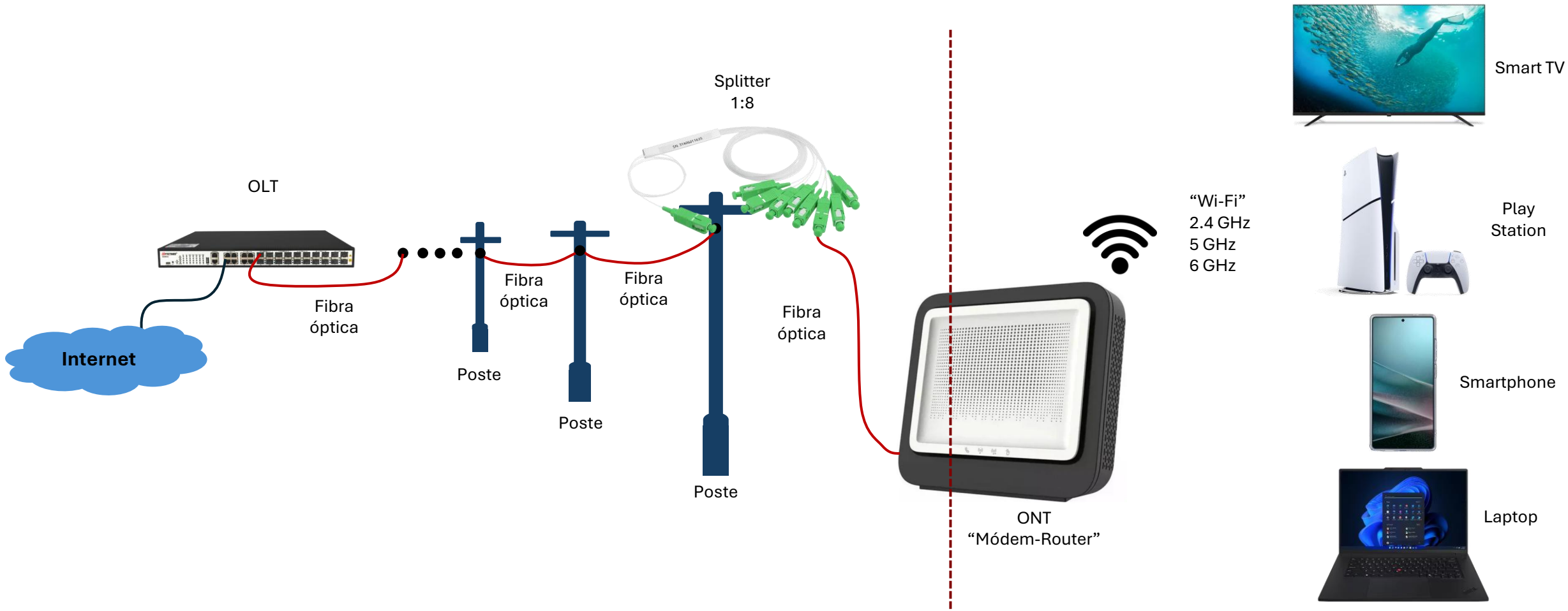
Ingeniería detrás de un ataque MITM mediante ARP Spoofing

Ing. Javier More Sanchez

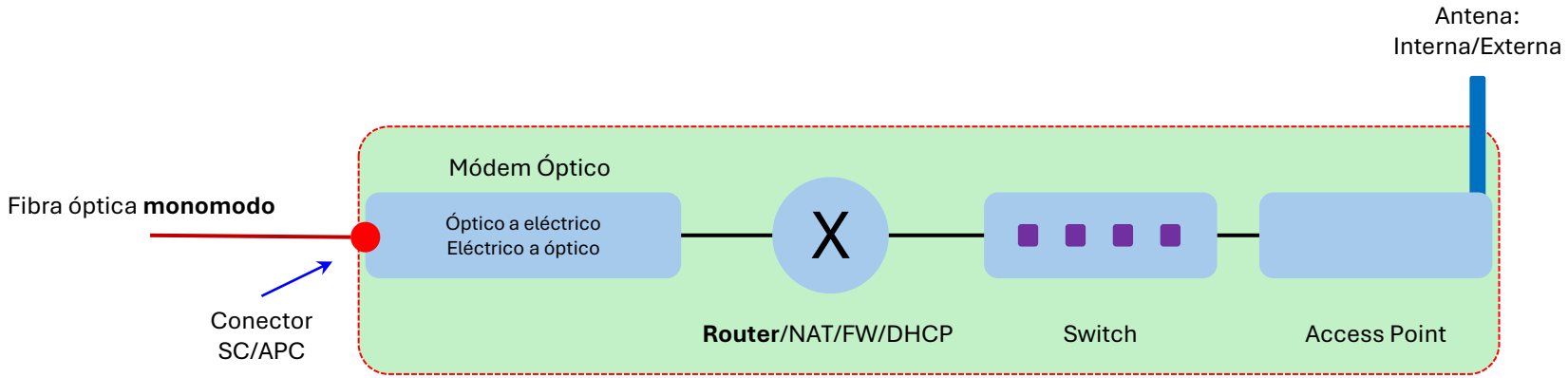
jmore@ulima.edu.pe

20 de noviembre de 2025

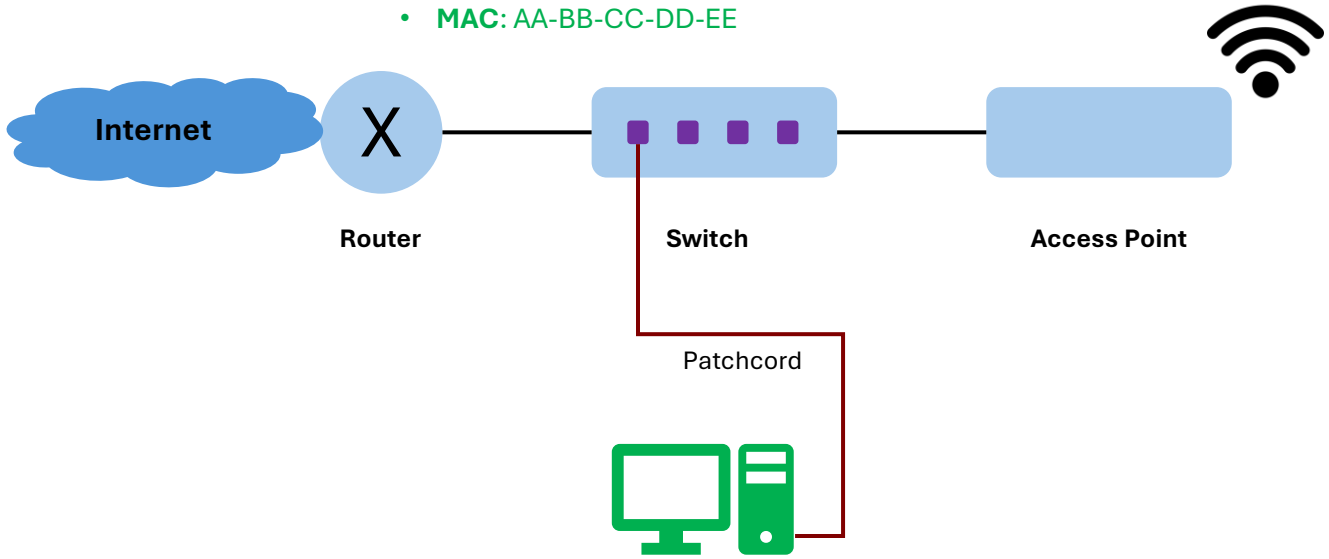
Así nos conectamos a Internet vía Fibra Óptica al Hogar (FTTH)



El “módem-router” tiene más funcionalidades



Tráfico normal en una LAN/WLAN

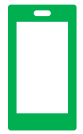


- **IP**: 192.168.1.1
- **MK**: 255.255.255.0
- **MAC**: AA-BB-CC-DD-EE

- **IP**: 192.168.1.10
- **MK**: 255.255.255.0
- **GW**: 192.168.1.1
- **MAC**: A1-B1-C1-D1-E1

Funcionamiento normal:
PC → Switch → Router → Red GPON → Internet (Servidor)

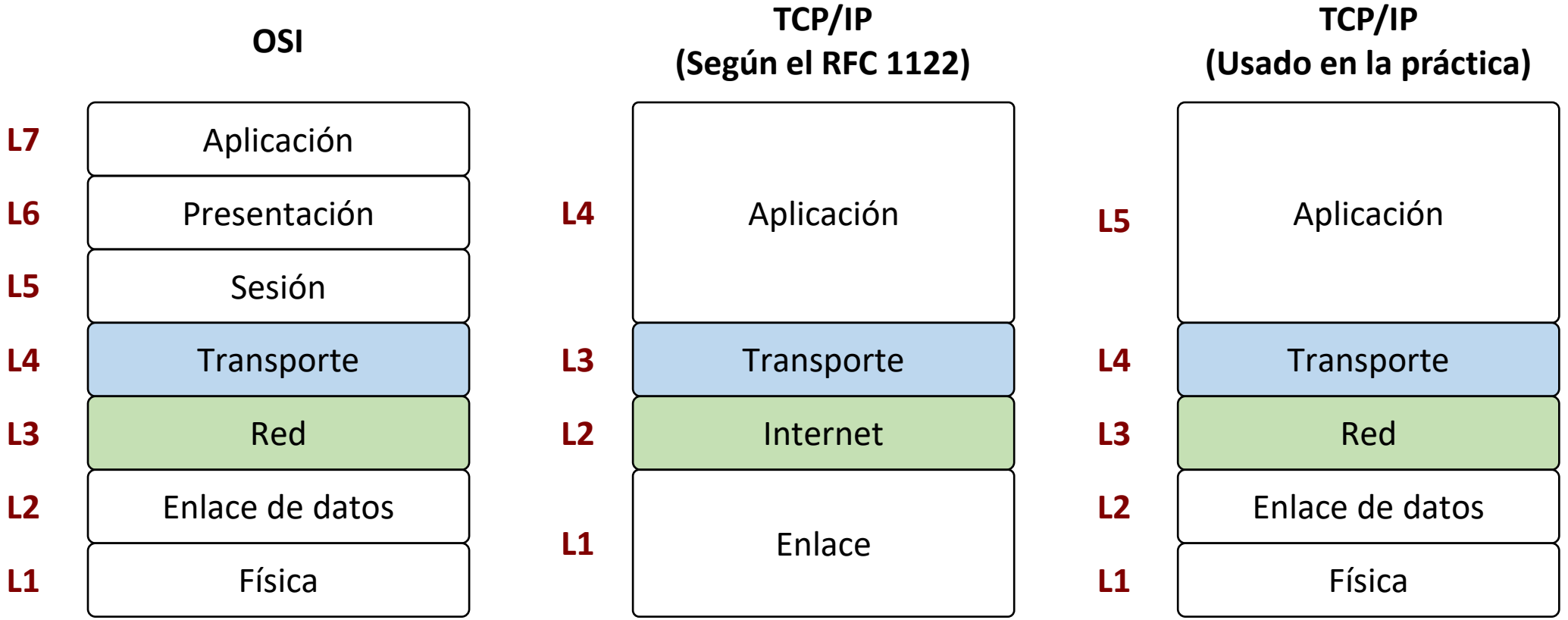
- **IP**: 192.168.1.11
- **MK**: 255.255.255.0
- **GW**: 192.168.1.1
- **MAC**: A2-B3-C4-D5-E6



- **IP**: 192.168.1.12
- **MK**: 255.255.255.0
- **GW**: 192.168.1.1
- **MAC**: A3-B3-C4-D5-E6

Funcionamiento normal:
Laptop → Access Point → Switch → Router → Red GPON → Internet (Servidor)

Recordando el modelo OSI y TCP/IP



- Desde 1984, el modelo OSI es estándar de la Organización Internacional de Normalización (**ISO**).
- Es un modelo teórico.

- En **1983** ya se usaba **TCP/IP** en ARPANET.
- El RFC 1122 se publicó en 1989.
- Su adopción fue masiva.

- En la práctica el modelo TCP/IP considera 5 capas.

Adaptado de Odom, W. (2024). *CCNA 200-301 Official Cert Guide, Volume 1 (2.ª ed.)*. Cisco Press.

El rol de Address Resolution Protocol (ARP)

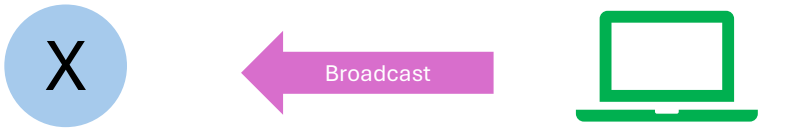
ARP es un protocolo usado para **mapear** direcciones **IPv4** (Capa 3) hacia direcciones **MAC** (Capa 2).

En mi PC (**192.168.1.35**) borraré la tabla ARP para forzar la captura en **Wireshark**

```
C:\Windows\System32>arp -d
```

```
24 3.657654    Intel_[redacted]    Broadcast    ARP    42 Who has 192.168.1.1? Tell 192.168.1.35
```

```
Ethernet II, Src: Intel_[redacted], Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Intel_[redacted]
  Type: ARP (0x0806)
  [Stream index: 2]
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Intel_[redacted]
  Sender IP address: 192.168.1.35
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1
```



Router: 192.168.1.1
Tarjeta de Red: AskeyCompute

Laptop: 192.168.1.35
Tarjeta de Red: INTEL

```
25 3.660325    AskeyCompute_[redacted]    Intel_[redacted]    ARP    46 192.168.1.1 is at [redacted]
```

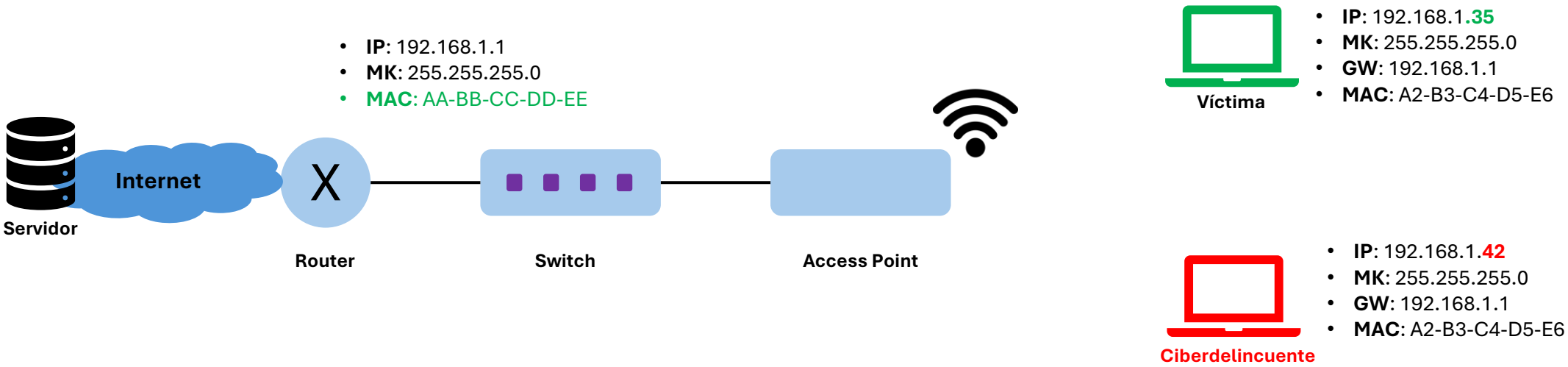
```
Ethernet II, Src: AskeyCompute_[redacted], Dst: Intel_[redacted]
  Destination: Intel_[redacted]
  Source: AskeyCompute_[redacted]
  Type: 802.1Q Virtual LAN (0x8100)
  [Stream index: 0]
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: AskeyCompute_[redacted]
  Sender IP address: 192.168.1.1
  Target MAC address: Intel_[redacted]
  Target IP address: 192.168.1.35
```

Router: 192.168.1.1
Tarjeta de Red: AskeyCompute

Laptop: 192.168.1.35
Tarjeta de Red: INTEL

```
Interfaz: 192.168.1.35 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1                    [redacted]            dinámico
```

¿Qué hay detrás de un ataque de “ARP Spoofing”?



IP ▲	MAC	Name	Vendor	Sent	Recvd
192.168.1.42	00:0c:29:f6:4f:54	eth0	VMware, Inc.	0 B	0 B
192.168.1.1	08	gateway	ASKEY COMPUTER CORP	1.5 kB	196 B
192.168.1.33	d4		Samsung Electronics Co.,Ltd	0 B	1.4 kB
192.168.1.34	a4		Seiko Epson Corporation	5.7 kB	6.0 kB
192.168.1.35	10		Intel Corporate	7.3 kB	1.4 kB
192.168.1.37	aa			1.4 kB	1.4 kB

Tabla ARP de la laptop víctima antes y después del ARP Spoofing

Ciberdelincuente

- **IP**: 192.168.1.**42**
- **MK**: 255.255.255.0
- **GW**: 192.168.1.1
- **MAC**: **00:0C:29:F6:4F:54**

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.42  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::d73a:34f1:c014:dfa2  prefixlen 64  scopeid 0x20<link>
        inet6 2001:1388:62a:a7ca:483:a890:8165:be04  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:f6:4f:54  txqueuelen 1000  (Ethernet)
        RX packets 53172  bytes 57226374 (54.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84980  bytes 5361189 (5.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Antes

```
Interfaz: 192.168.1.35 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1            08-33[redacted]    dinámico
```

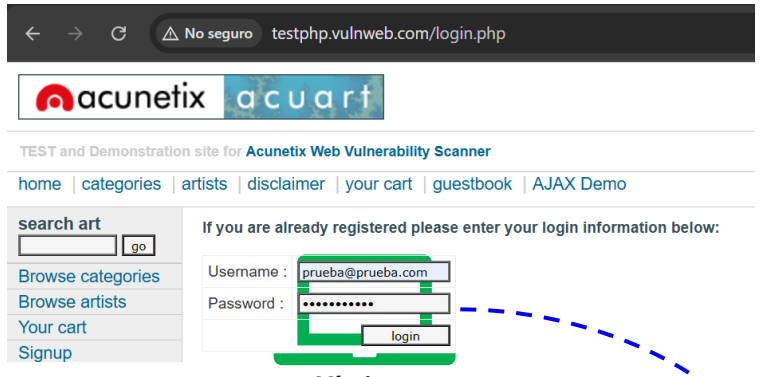
Víctima

- **IP**: 192.168.1.**35**
- **MK**: 255.255.255.0
- **GW**: 192.168.1.1

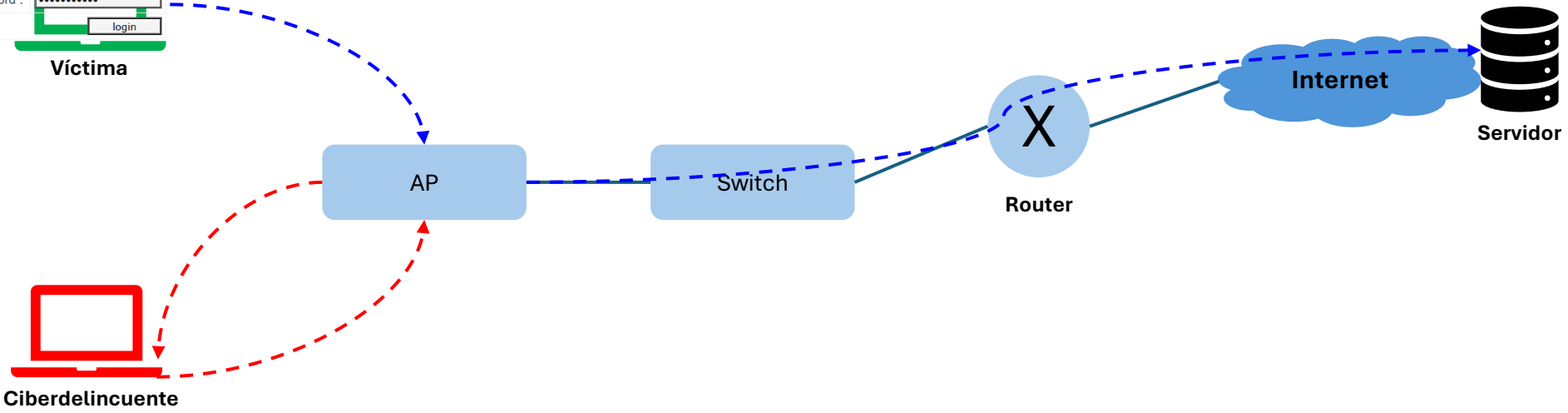
Después

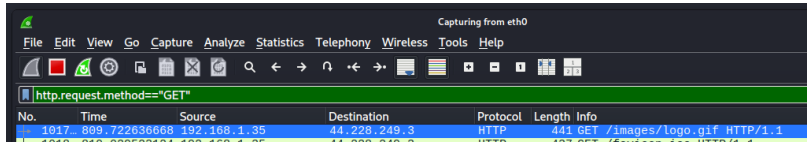
```
Interfaz: 192.168.1.35 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1            00-0c-29-f6-4f-54     dinámico
```

Ruta de los bits bajo un esquema de ARP Spoofing



Víctima





Marco legal peruano

Ley Nº 30096: Ley de delitos informáticos

Artículo 2. Acceso ilícito
El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad **no menor de uno ni mayor de cuatro años** y con treinta a noventa días-multa.
Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa".

Artículo 3. Atentado a la integridad de datos informáticos
El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad **no menor de tres ni mayor de seis años** y con ochenta a ciento veinte días-multa.

Artículo 7. Interceptación de datos informáticos
El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las **emisiones electromagnéticas** provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad **no menor de tres ni mayor de seis años**.

Ley actualizada disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1088463

Javier More Sanchez

Ing. Electrónico | Mag. Telecomunicaciones | Mag. Regulación SSPP | Ms. Gestión de Infraestructuras

Peru · Contact info

Universidad de Lima

Universidad Nacional Mayor de San Marcos

Gracias