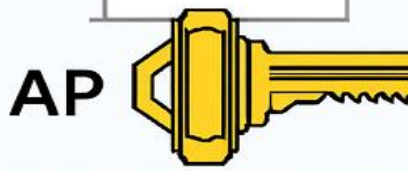
WiFi: El arte de la intercepción

Las pruebas de penetración de aplicaciones móviles son un enfoque proactivo para mejorar la seguridad de las aplicaciones móviles mediante la identificación y el abordaje de posibles amenazas.

4-Way Handshake



Pick Random ANonce

EAPOL-Key(Reply Required, Unicast, ANonce) M1

Pick Random SNonce, Derive PTK = 802.11i-PRF(PMK, ANonce
SNonce || AP MAC Addr || STA RSN IE)

M2

EAPOL-Key(Unicast, SNonce, MIC, STA RSN IE

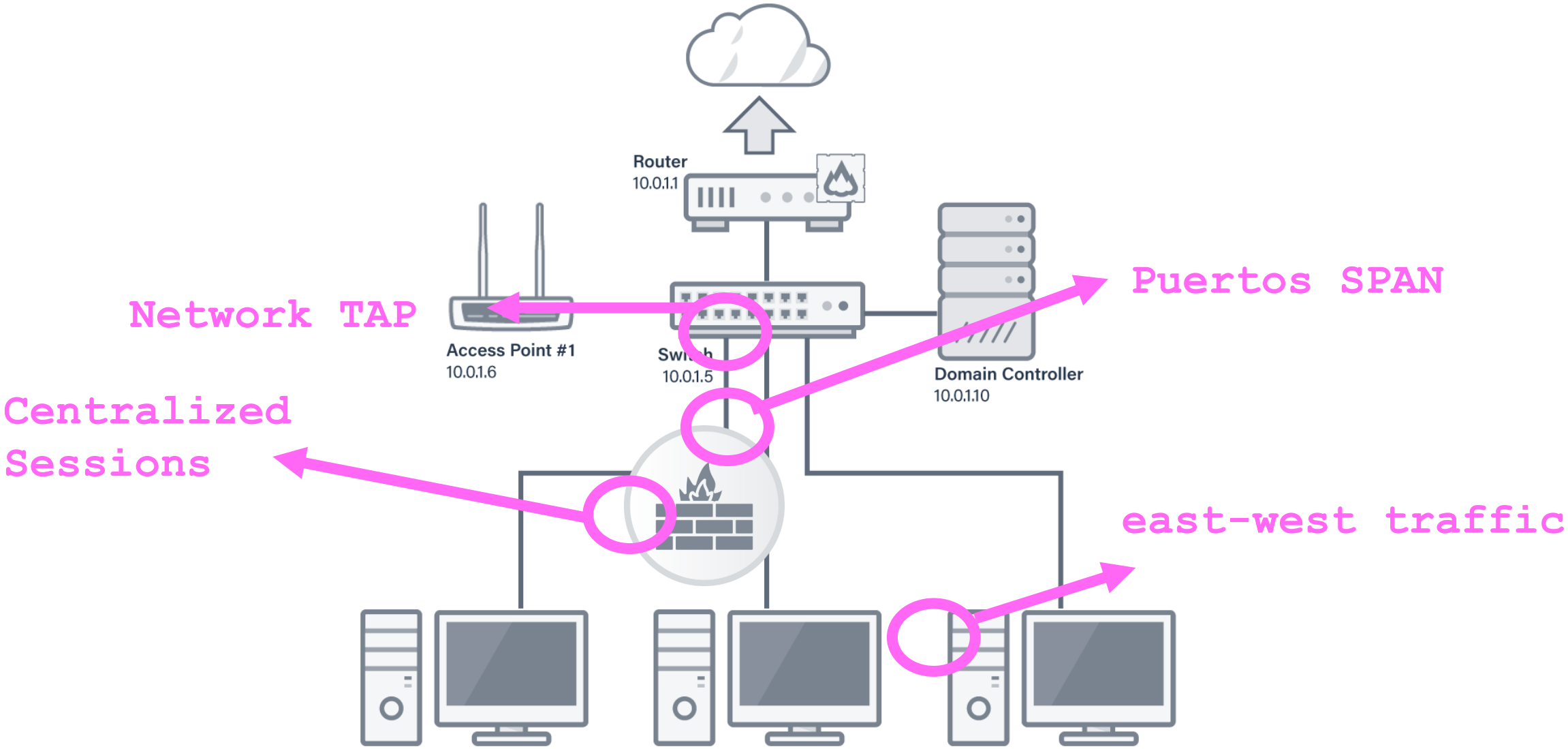
Derive PTK

EAPOL-Key(Reply ıquired, lnſlall P1 N M4

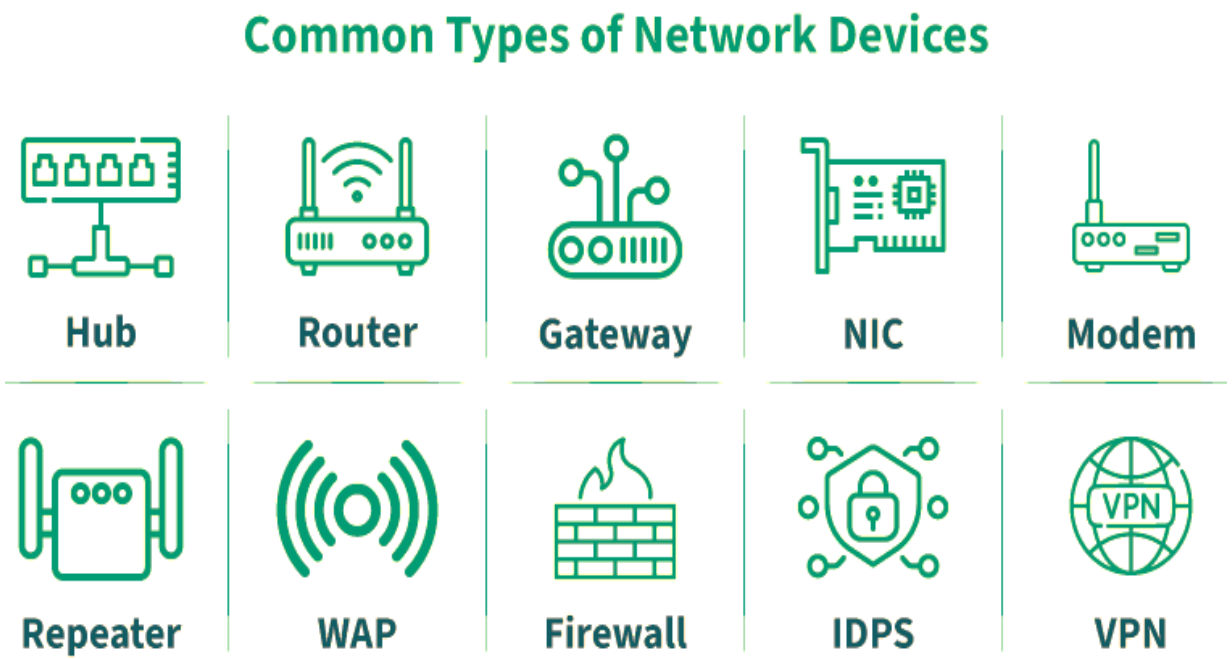
M4

EAPOL-Key(Unicast)

Análisis de tráfico en red



Análisis de tráfico en red



METADATOS

LOGS

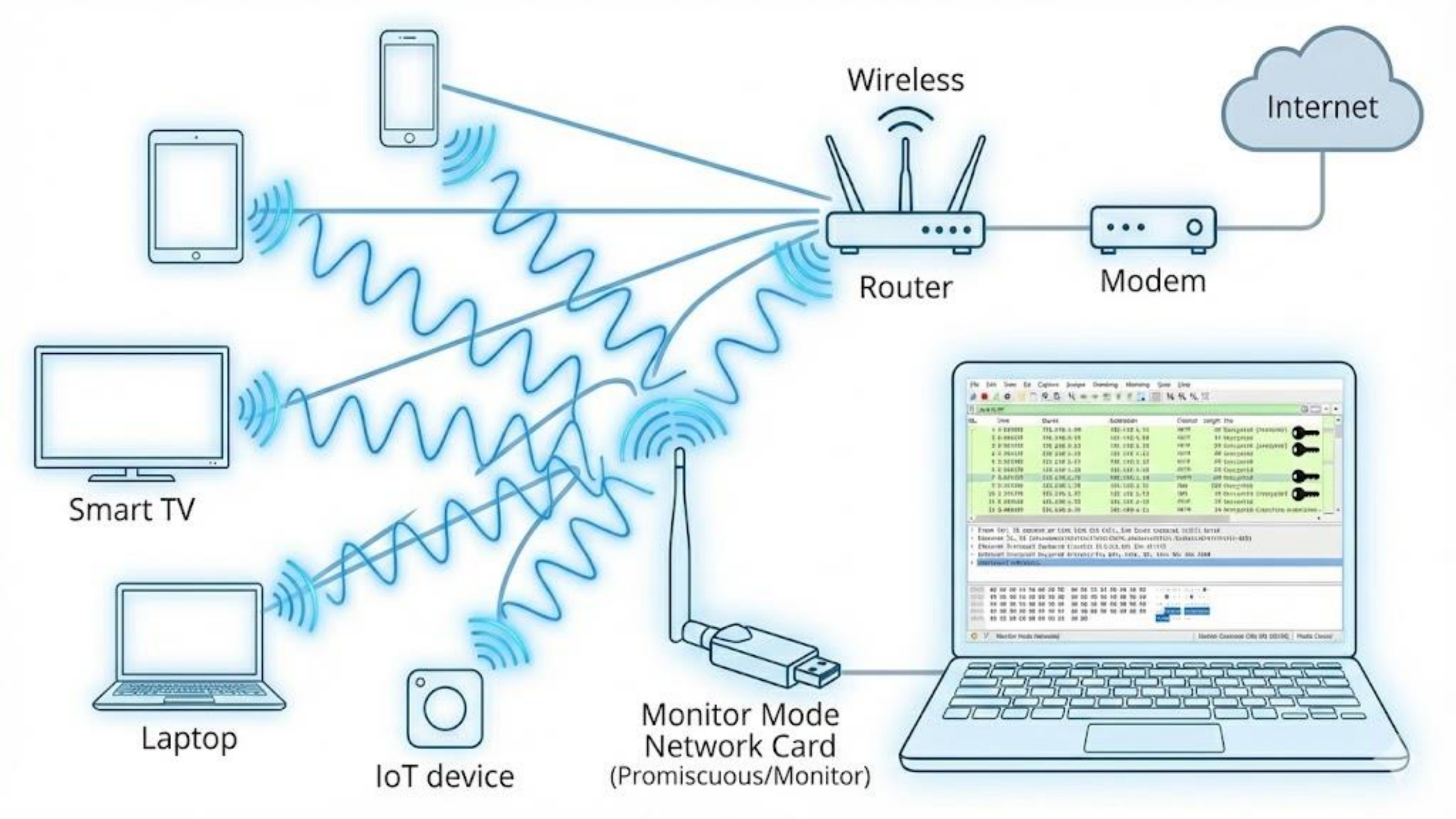
TRANSFERENCIAS DE ARCHIVOS

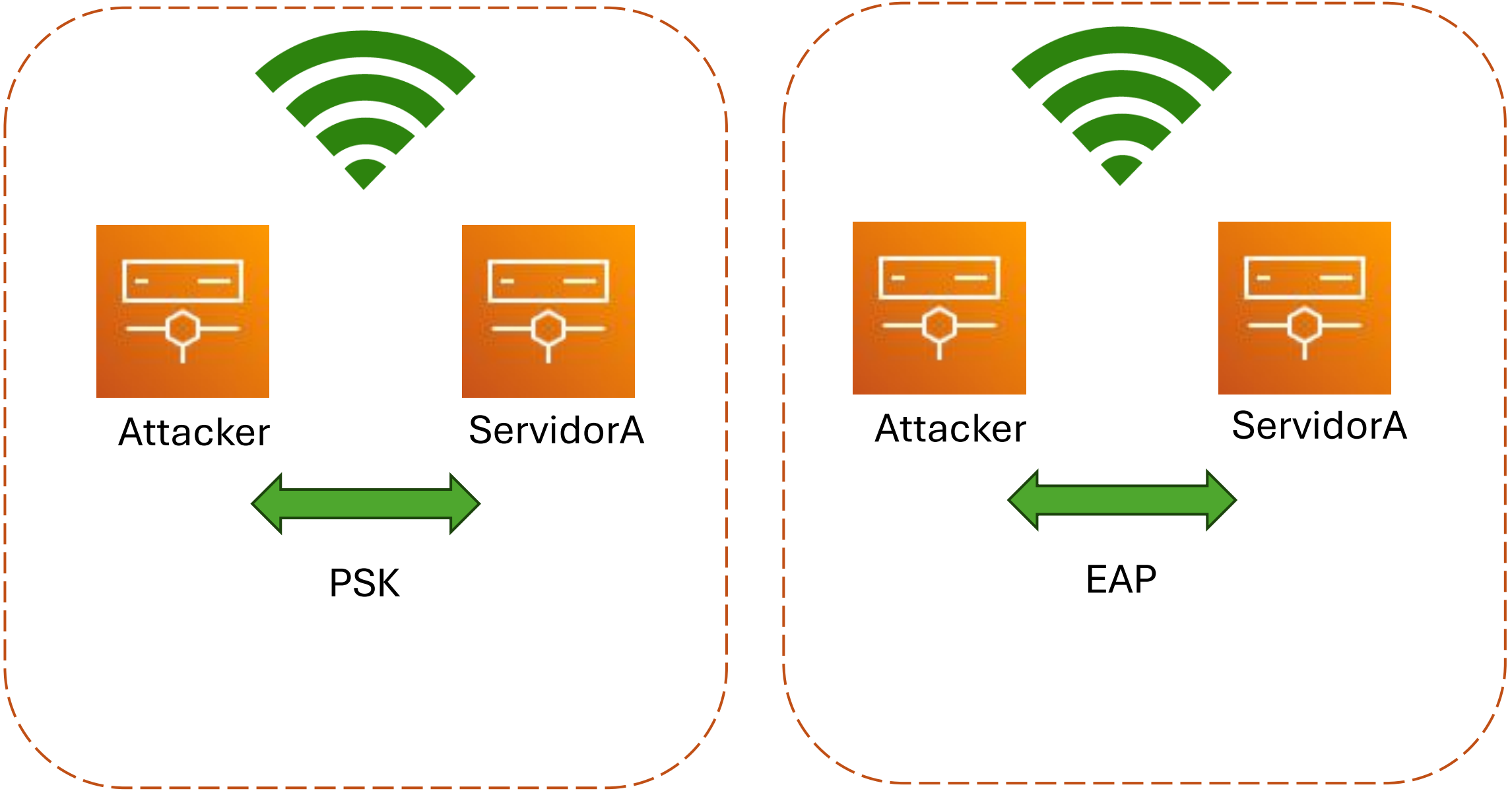
RECONSTRUCCION DE SESIONES

FLUJOS DE RED

PUNTOS DE COLECTA

Laboratorio & Herramientas


Wireless
Internet
Router
Modem
Smart TV
Laptop
IoT device
Monitor Mode
Network Card
(Promiscuous/Monitor)


Attacker
ServidorA
PSK
Attacker
ServidorA
EAP

Código

```
#Instalación de cabeceras

$ uname -r
$ apt search linux-headers-$(uname -r)
$ ls -l /usr/src/linux-headers-$(uname -r)
$ sudo apt update
$ sudo apt install linux-headers-$(uname -r)
$ ls -l /usr/src/linux-headers-$(uname -r)
```

Recomendaciones para remediación o prevención

- Utilizar la validación de direcciones de origen y la protección contra spoofing.
- Establecer procedimientos de emergencia para que su
- Distribuir servicios públicos (Anycast, múltiples POP, balanceo de carga multirregión)
- Desarrollar un manual de estrategias DDoS y realizar simulacros de simulación