

# Privacidad en WiFi mediante WPA2-Personal



# Privacidad WiFi con WPA2/PSK

WPA-Personal (WiFi Protected Access)





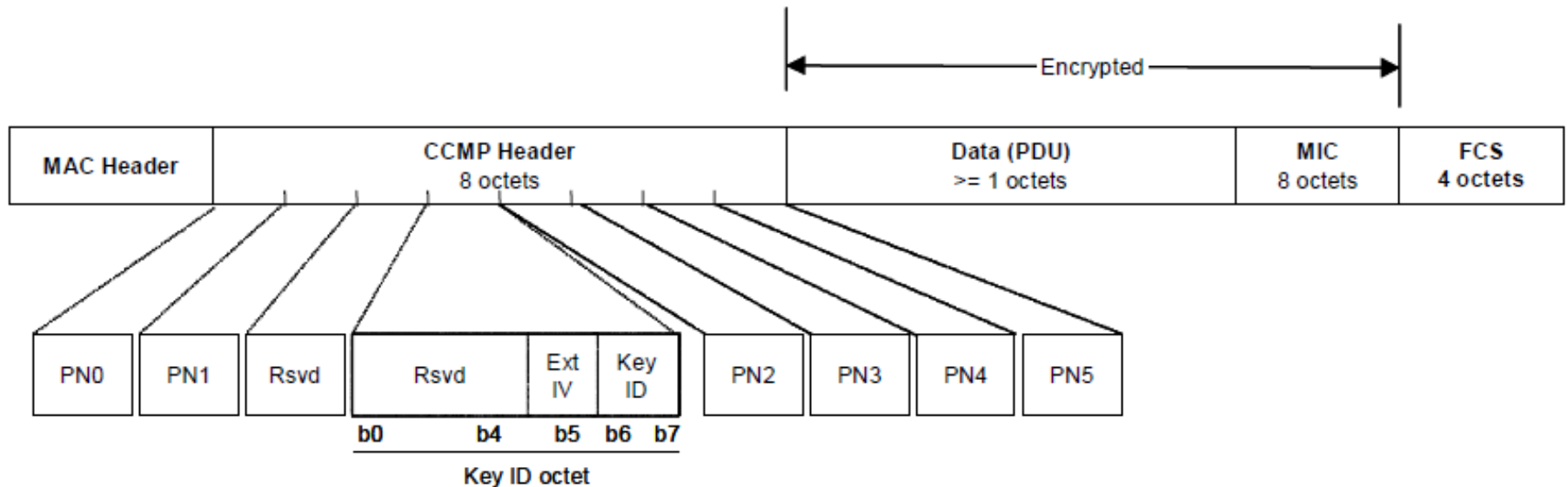
# Privacidad WiFi con WPA2/PSK

CCMP – CTR with CBC-MAC Protocol

- **CounTeR** mode
- **Cipher-Block Chaining** with **Message Authentication Code**

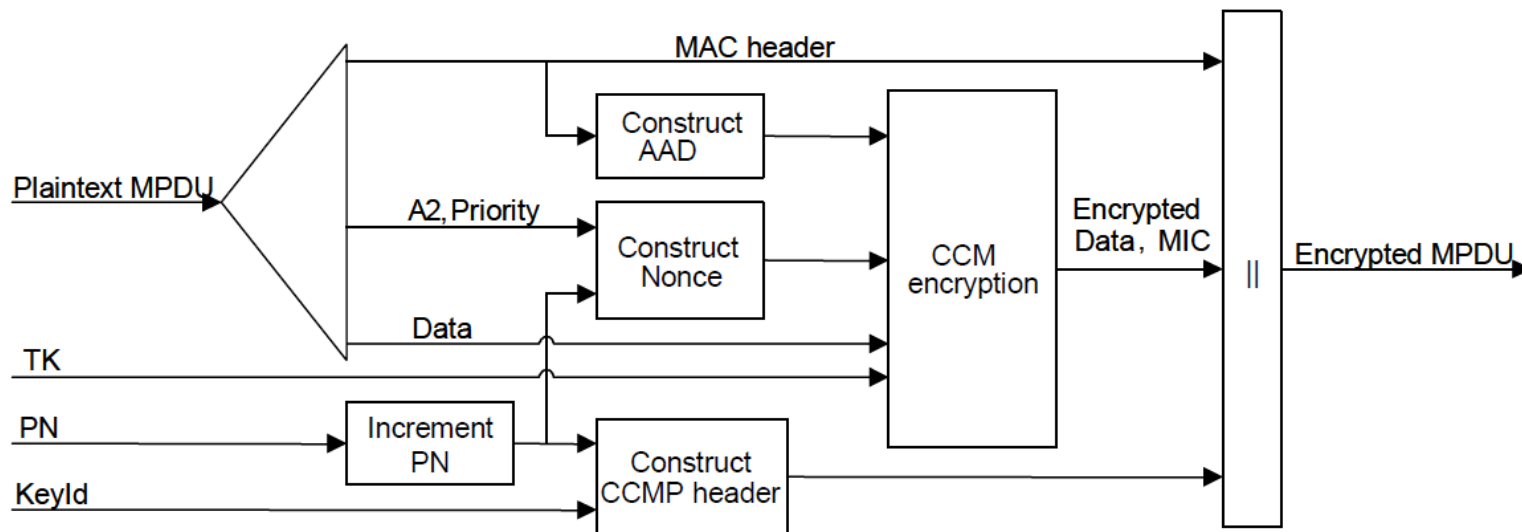
# Privacidad WiFi con WPA2/PSK

## CCMP – MPDU expandida



# Privacidad WiFi con WPA2/PSK

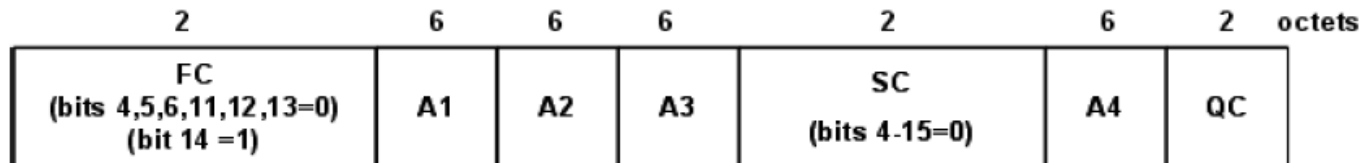
## CCMP – Proceso de encapsulado



# Privacidad WiFi con WPA2/PSK

## CCMP – Proceso de encapsulado

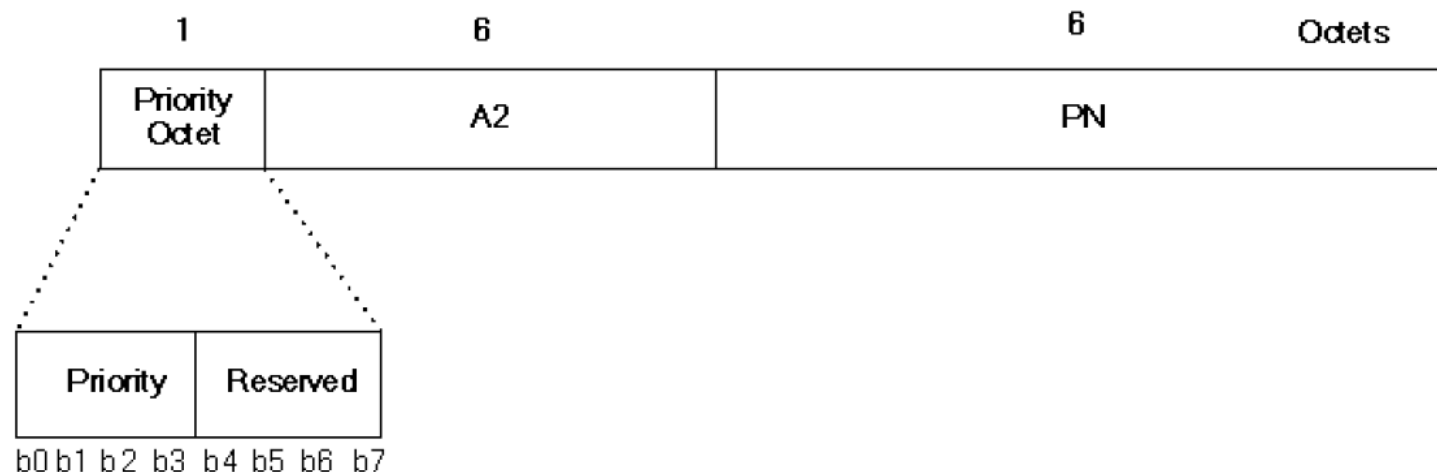
### ■ Additional Authentication Data



# Privacidad WiFi con WPA2/PSK

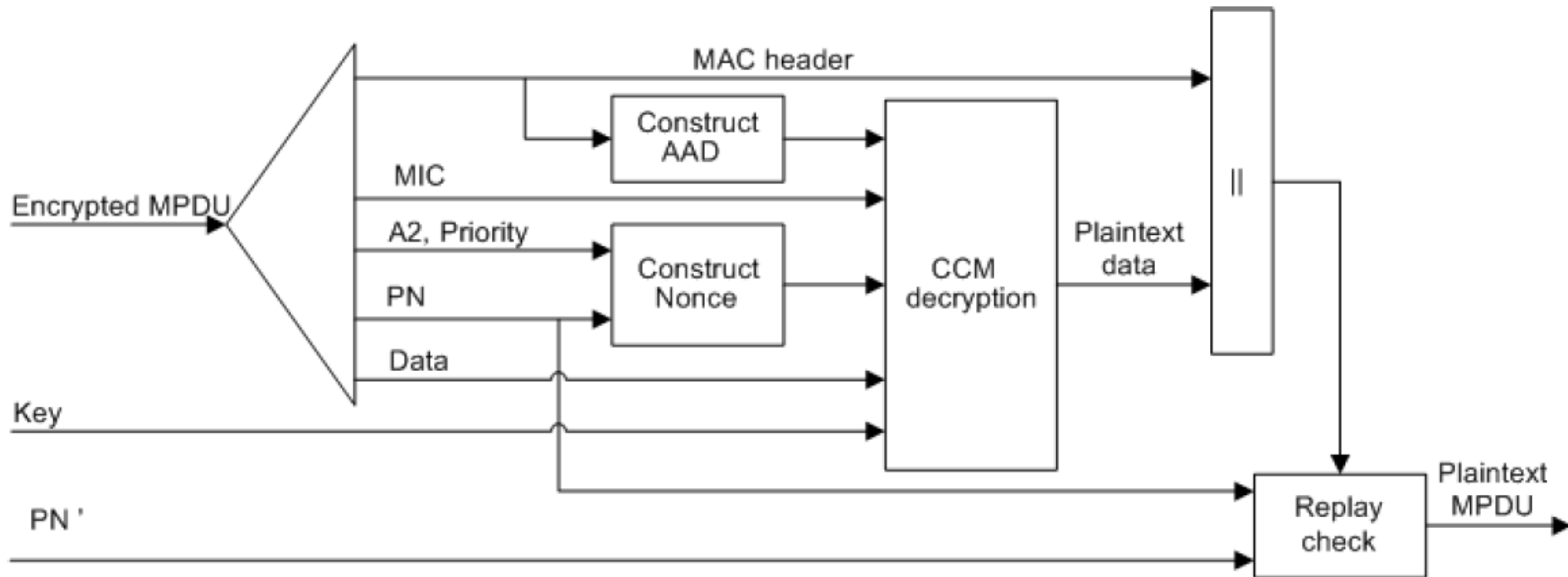
## CCMP – Proceso de encapsulado

- CCM Nonce (number used once)



# Privacidad WiFi con WPA2/PSK

## CCMP – Proceso de desencapsulado





# Privacidad WiFi con WPA2/PSK

## AES – Advanced Encryption Standard

- Estándar de cifrado en USA

  - FIPS PUB 197

- Rijndael

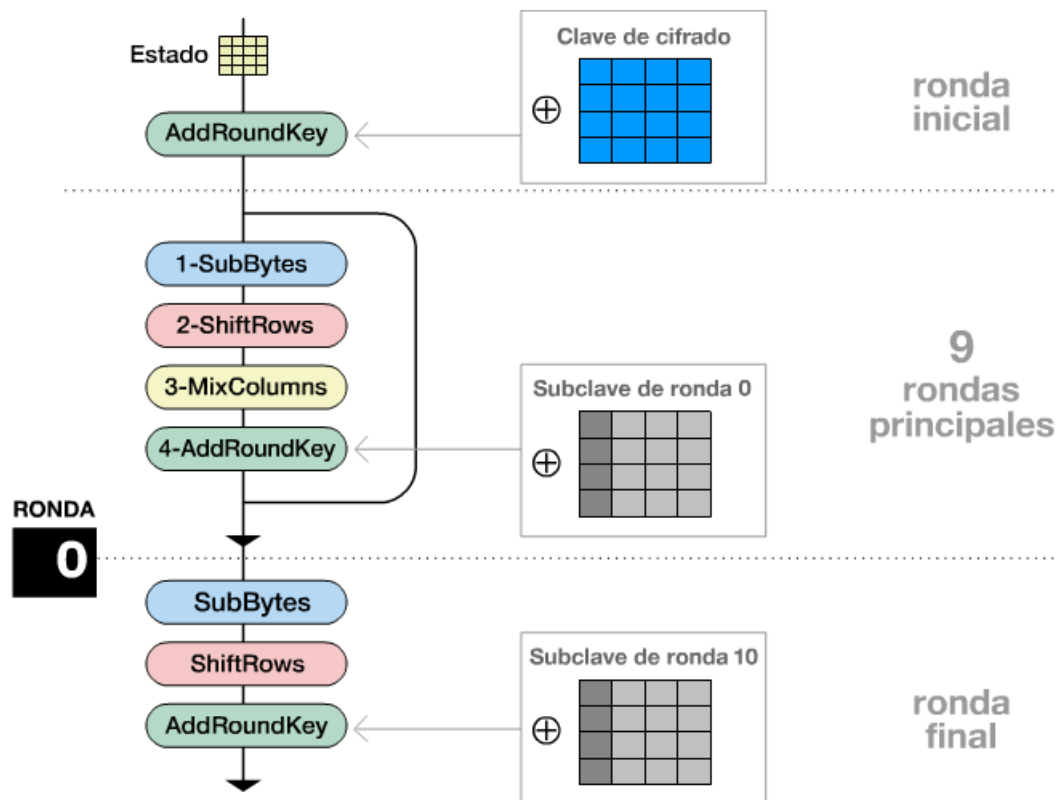
- Fases

  - SubBytes

  - ShiftRows

  - MixColumns

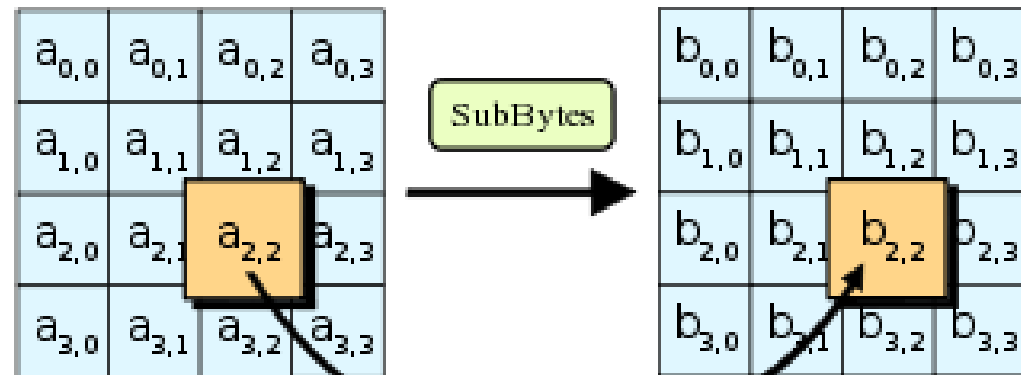
  - AddRoundKey



# Privacidad WiFi con WPA2/PSK

## AES – Advanced Encryption Standard

### ■ SubBytes

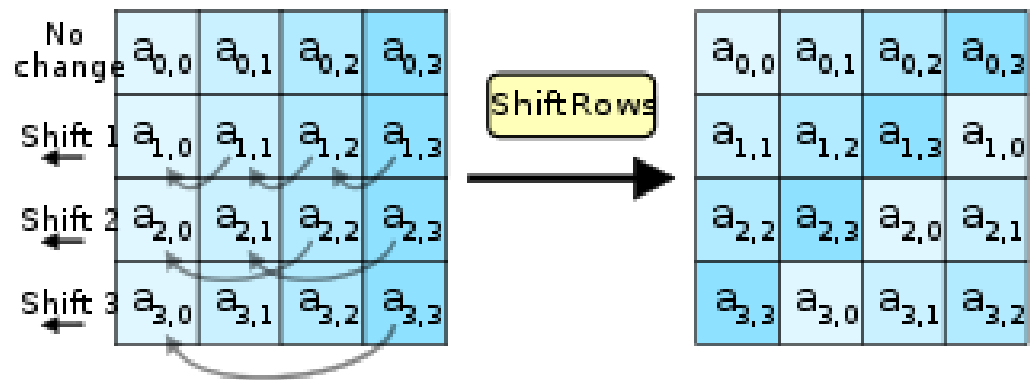


		y															
hex		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

# Privacidad WiFi con WPA2/PSK

## AES – Advanced Encryption Standard

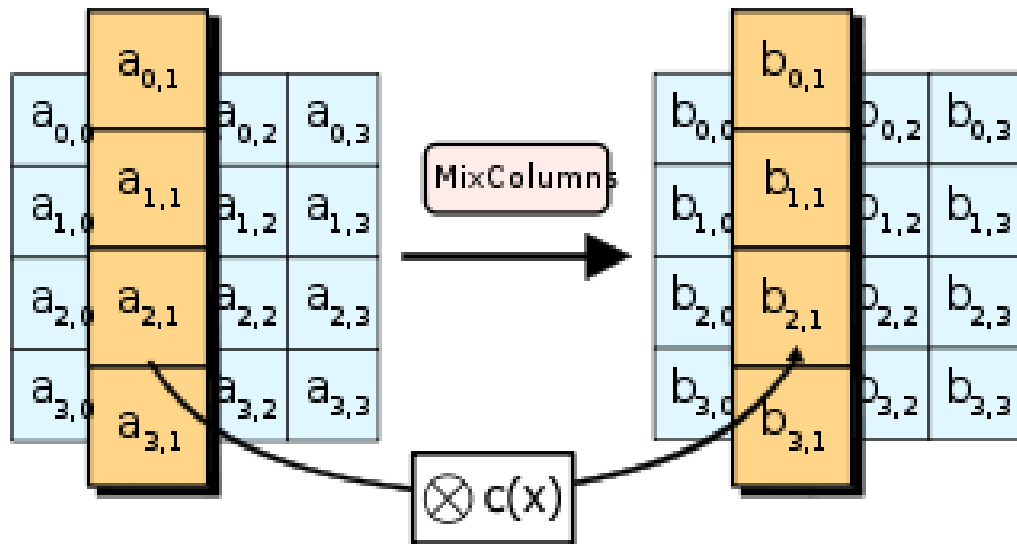
### ■ ShiftRows



# Privacidad WiFi con WPA2/PSK

## AES – Advanced Encryption Standard

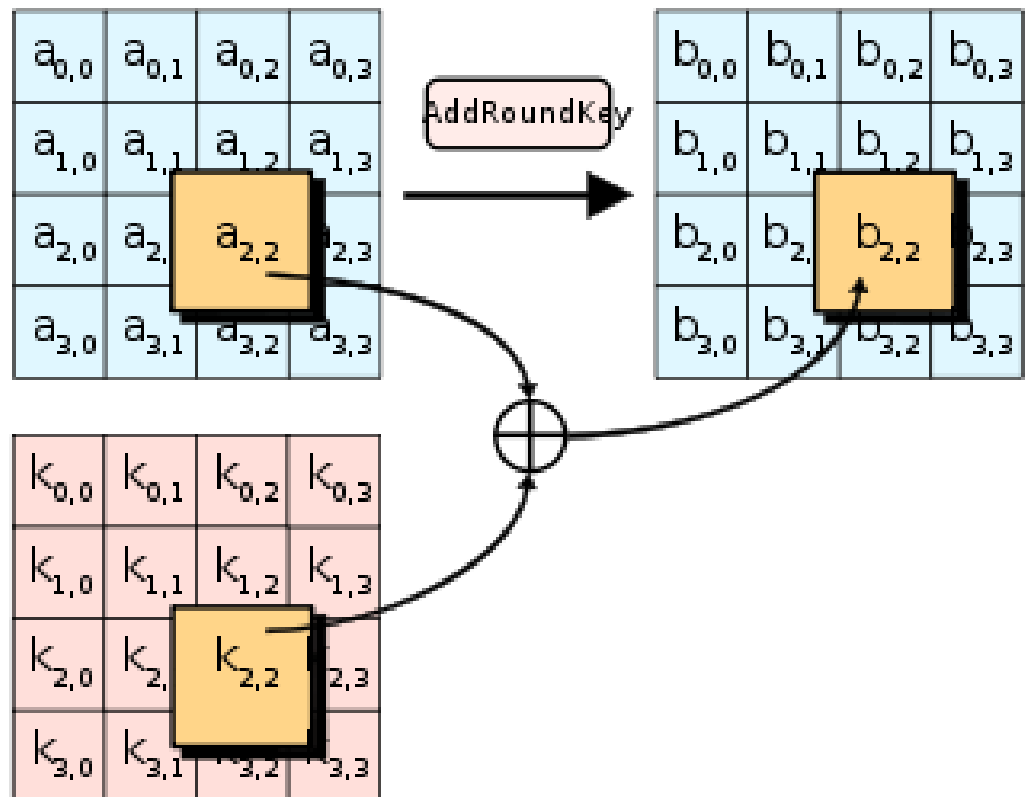
### ■ MixColumns



# Privacidad WiFi con WPA2/PSK

## AES – Advanced Encryption Standard

### ■ AddRoundKey



# Privacidad WiFi con WPA2/PSK

AP con seguridad WPA2-Personal

Small Business  
cisco WAP4410N Wireless-N Access Point with Power Over

Setup

Wireless

- Basic Settings
- Security
- Connection Control
- Wi-Fi Protected Setup
- VLAN and QoS
- Advanced Settings

AP Mode

Administration

Status

### Wireless Security

Select SSID: WiFiWPA2 ▼

Wireless Isolation:(between SSID) ☐ Enabled ☒ Disabled

Security Mode: WPA2-Personal ▼

Wireless Isolation:(within SSID) ☐ Enabled ☒ Disabled

WPA Algorithm: AES

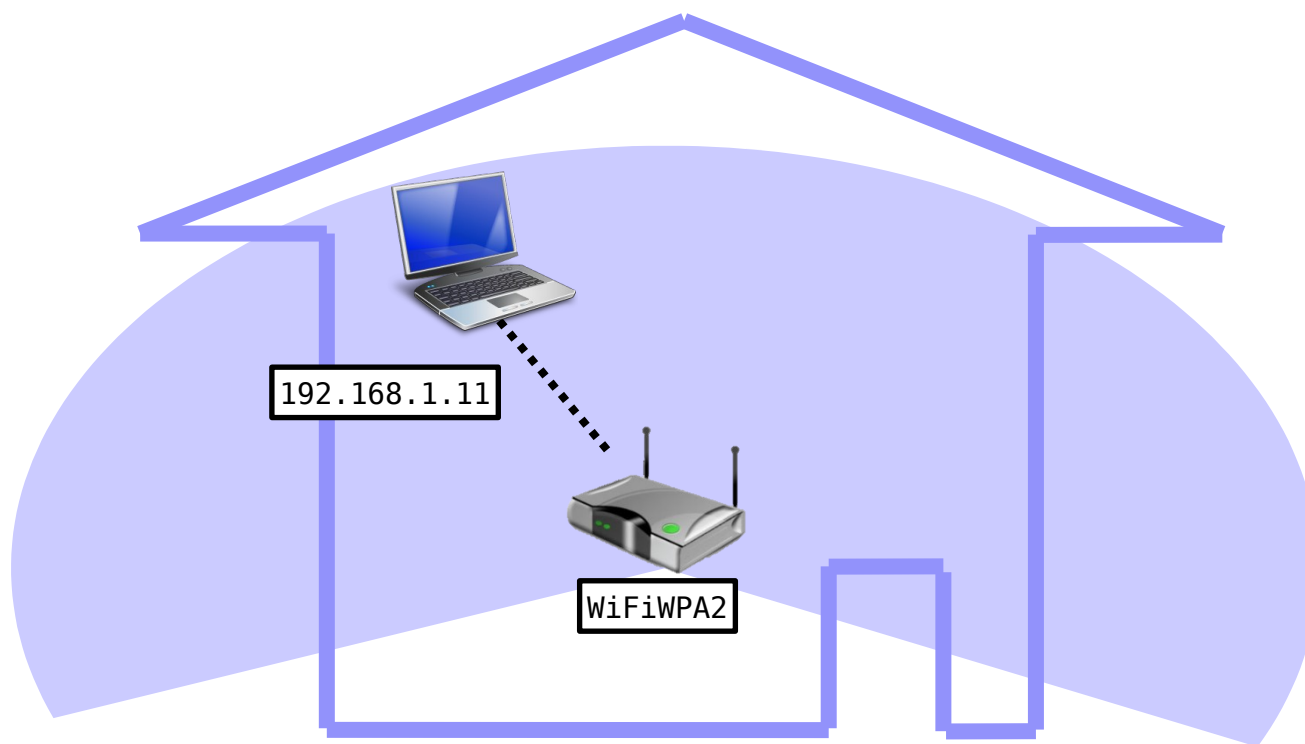
Pre-shared Key: clavesecreta

Key Renewal: 3600 seconds

Save Cancel

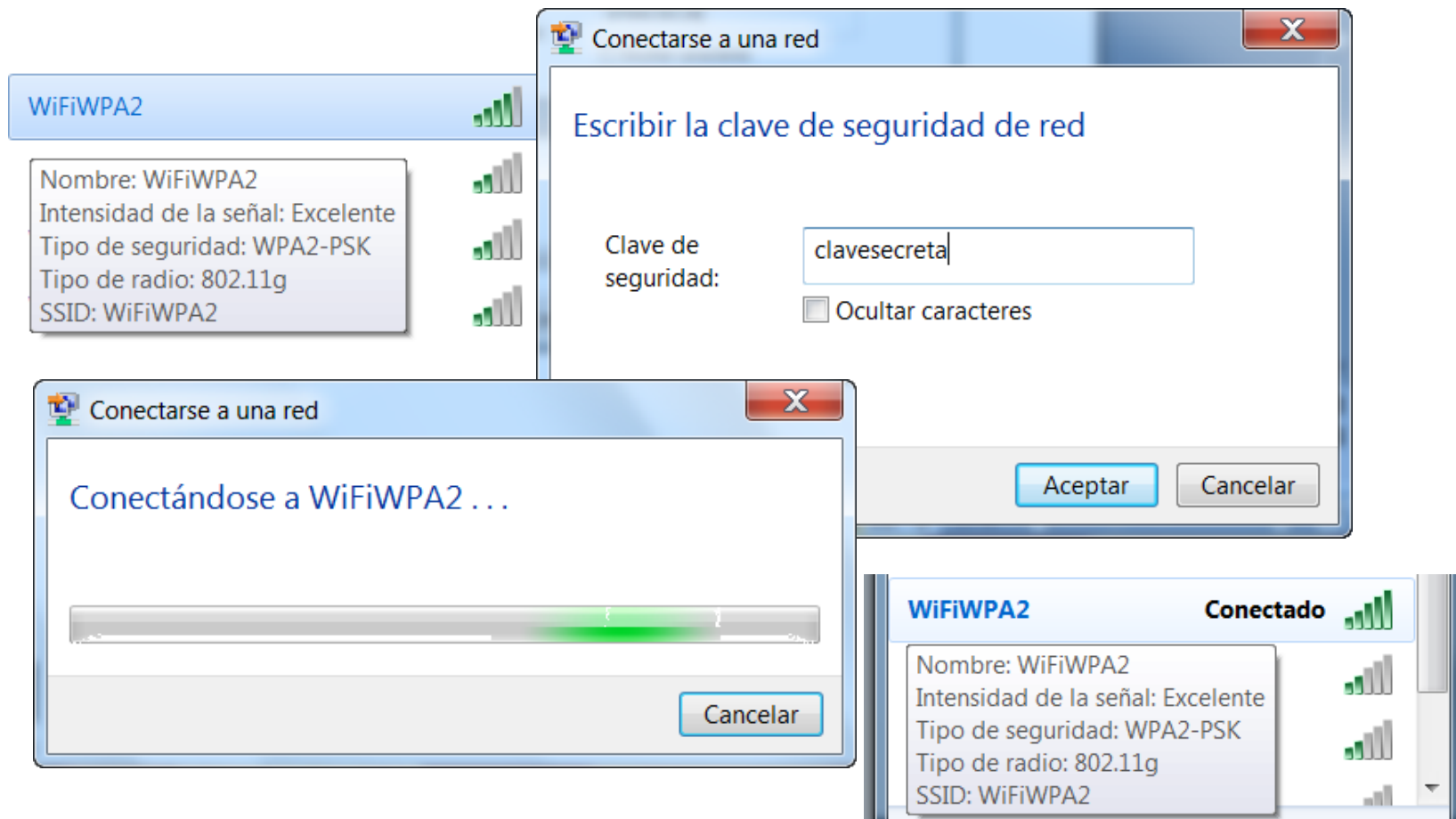
# Privacidad WiFi con WPA2/PSK

Conexión Windows a AP con WPA2-Personal



# Privacidad WiFi con WPA2/PSK

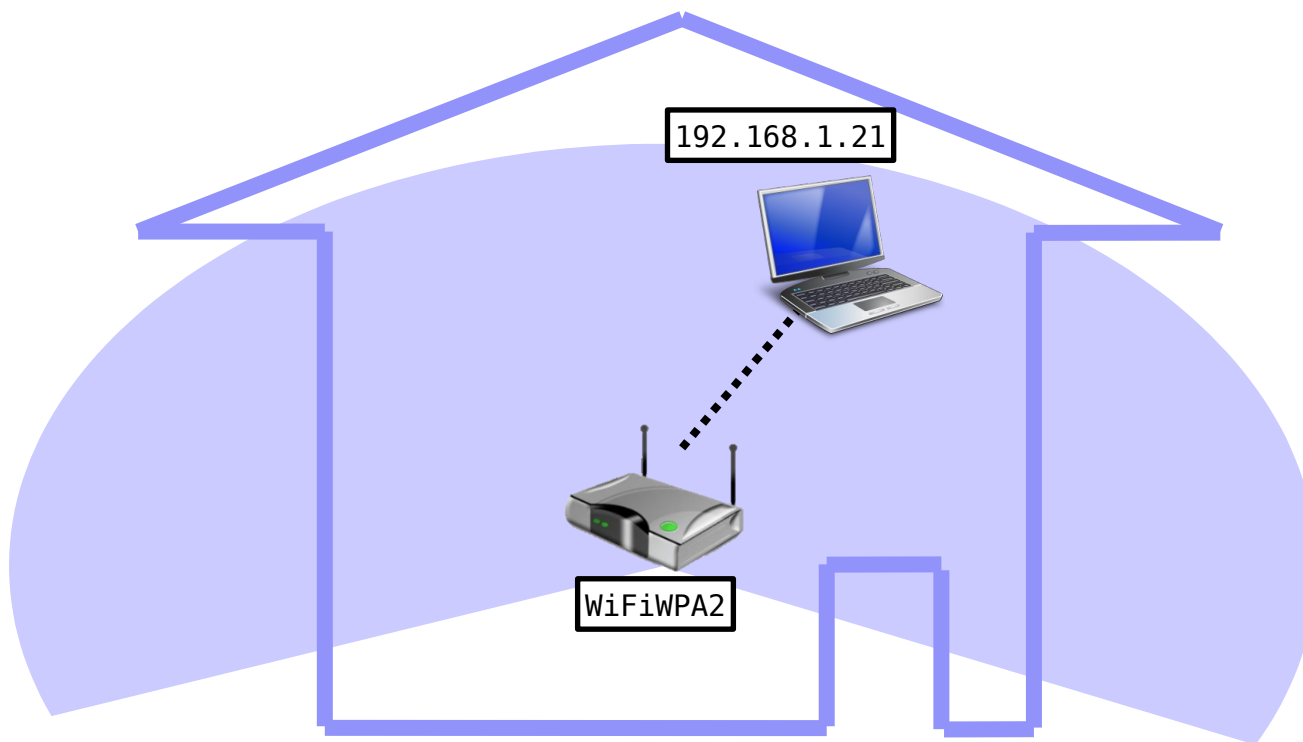
## Conexión Windows a AP con WPA2-Personal





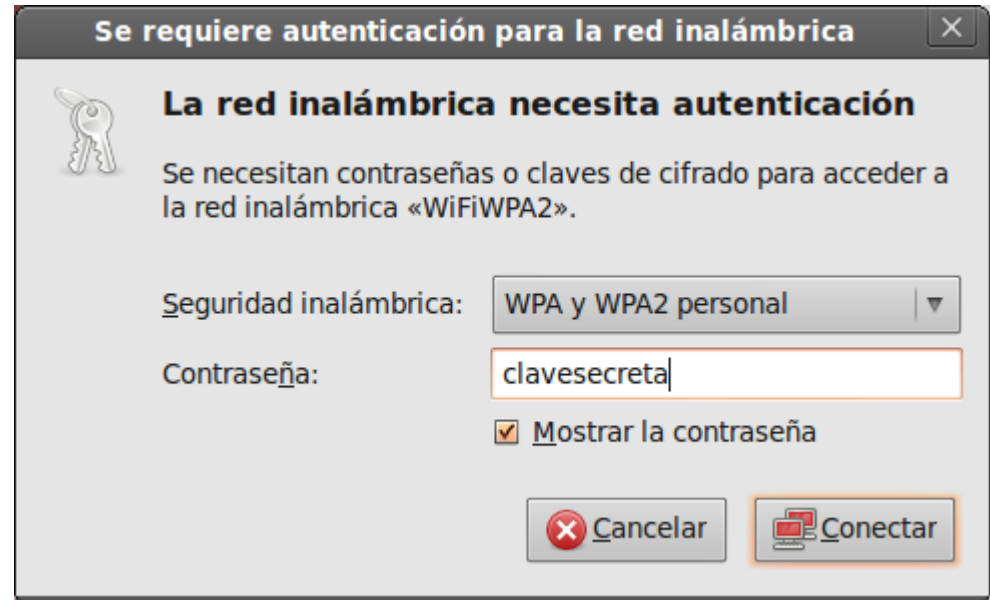
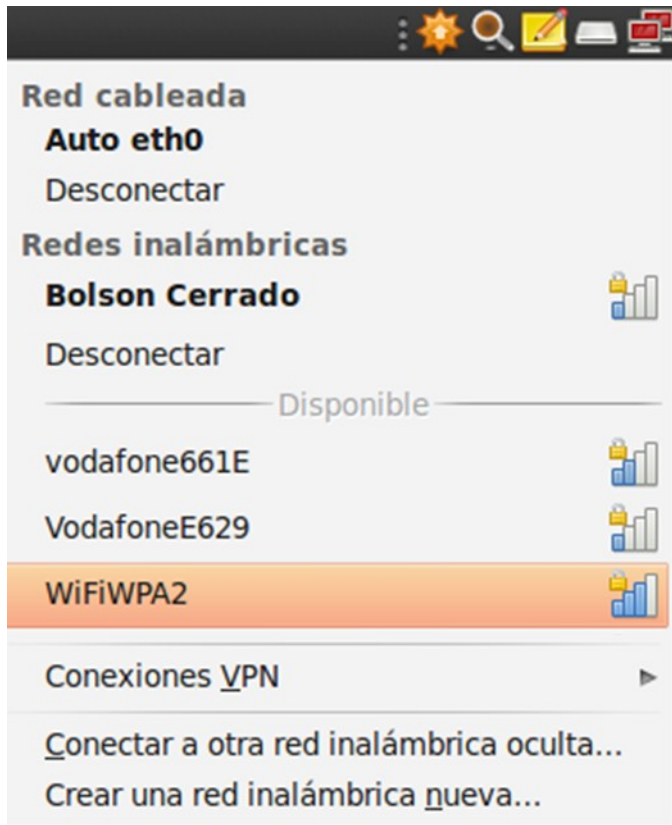
# Privacidad WiFi con WPA2/PSK

Conexión desde Linux a AP con WPA2-PSK



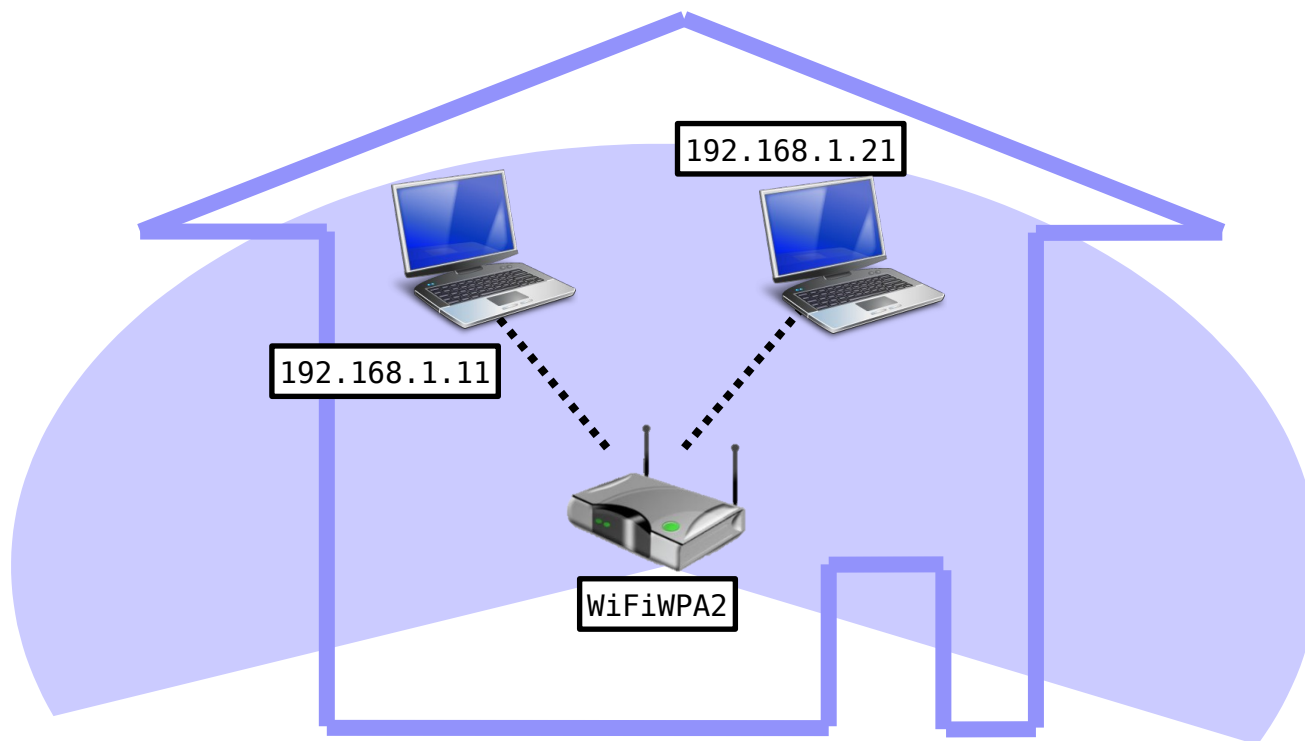
# Privacidad WiFi con WPA2/PSK

## Conexión desde Linux a AP con WPA



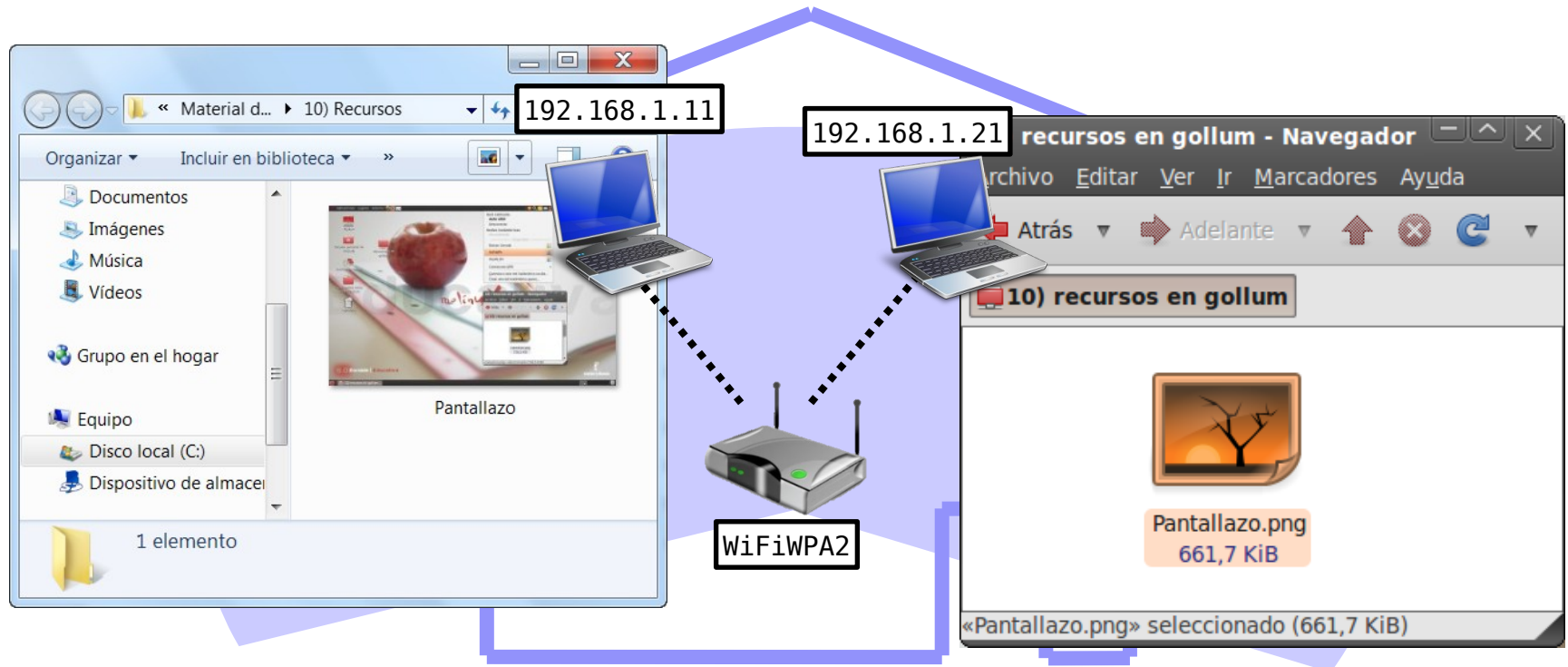
# Privacidad WiFi con WPA2/PSK

Montaje a realizar



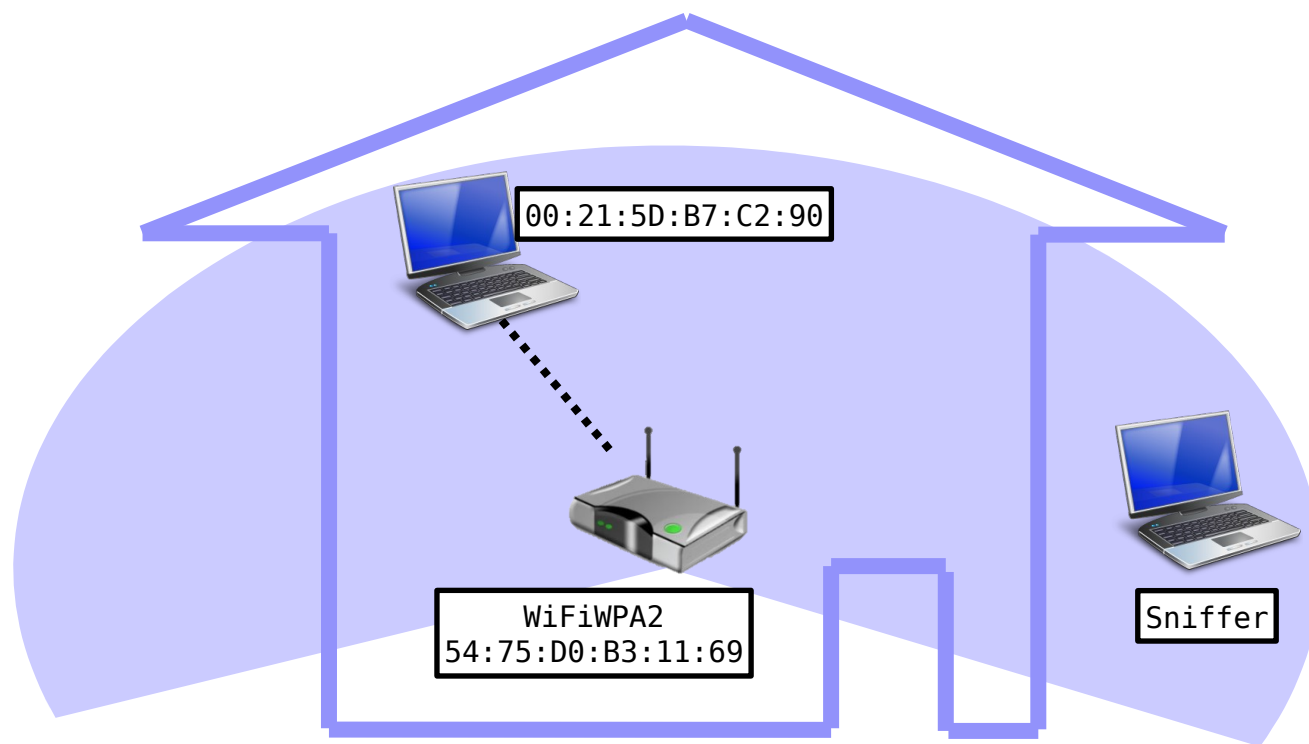
# Privacidad WiFi con WPA2/PSK

## Pruebas de conectividad



# Privacidad WiFi con WPA2/PSK

Montaje a realizar



# Privacidad WiFi con WPA2/PSK

## Monitorización de IVs con WireShark

