

\$ W7 · 5GC NETWORK FUNCTIONS

➤ OTHER NFS

NRF、SCP、AUSF、UDM、UDR、PCF、BSF、CHF、NSSF、NEF —— 以及獨立
一講的非 3GPP 接入

/> 課程大綱

PART A · 其他網路元件

PART B · 獨立一講

01

SBA

生產者與消費者

02

NRF

註冊、發現、
Token

03

SCP

間接通訊代理

04

AUSF

5G-AKA 認證

05

**UDM /
UDR**

資料與
Webconsole

B

**NON-
3GPP**

N3IWF · TNGF ·
TWIF · ATSSS

06

PCF

策略中樞

07

BSF

Session ↔ PCF
綁定

08

CHF

計費與配額

09

NSSF

網路切片選擇

10

NEF

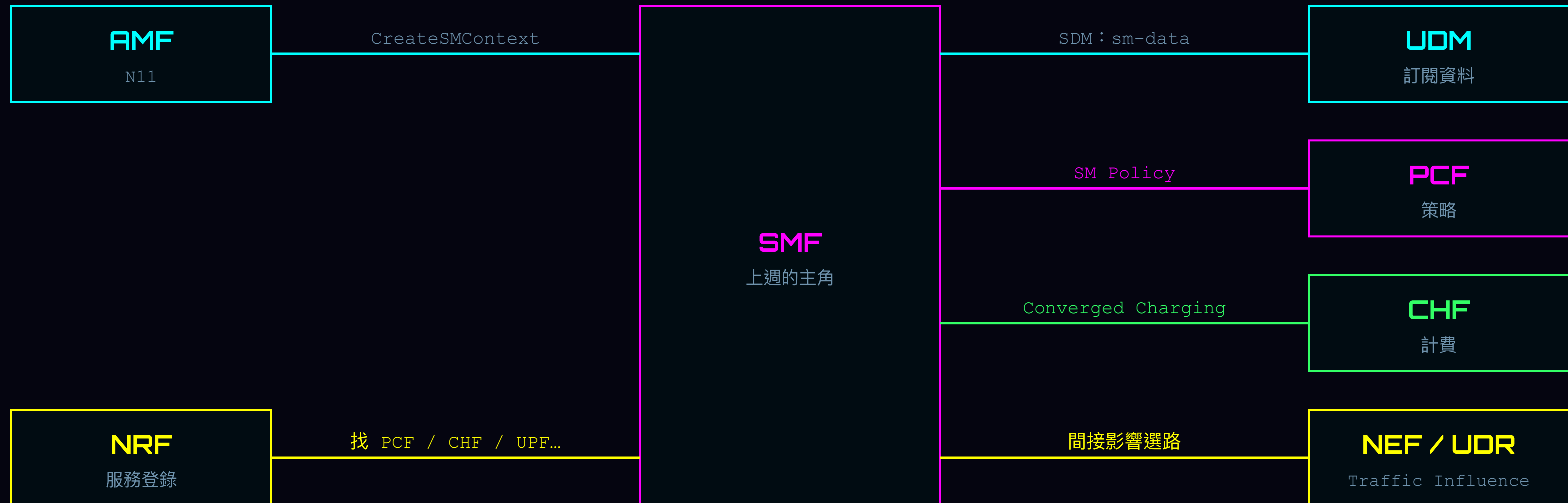
能力對外開放

\$ RECAP · W6

／> SMF / UPF 回顧

上週 SMF 呼叫過的那些 NF，就是今天的主角

➤ 上週 SMF 呼叫過誰？



上週把這些 NF 當黑盒子；今天逐一打開。

➤ 今天的 NF 地圖

服務治理

NRF

登錄與發現

SCP

轉送代理

身分與資料

AUSF

認證

UDM

用戶資料邏輯

UDR

統一資料庫

策略與計費

PCF

策略

BSF

綁定

CHF

計費

切片與開放

NSSF

切片選擇

NEF

能力開放

非 3GPP

N3IWF

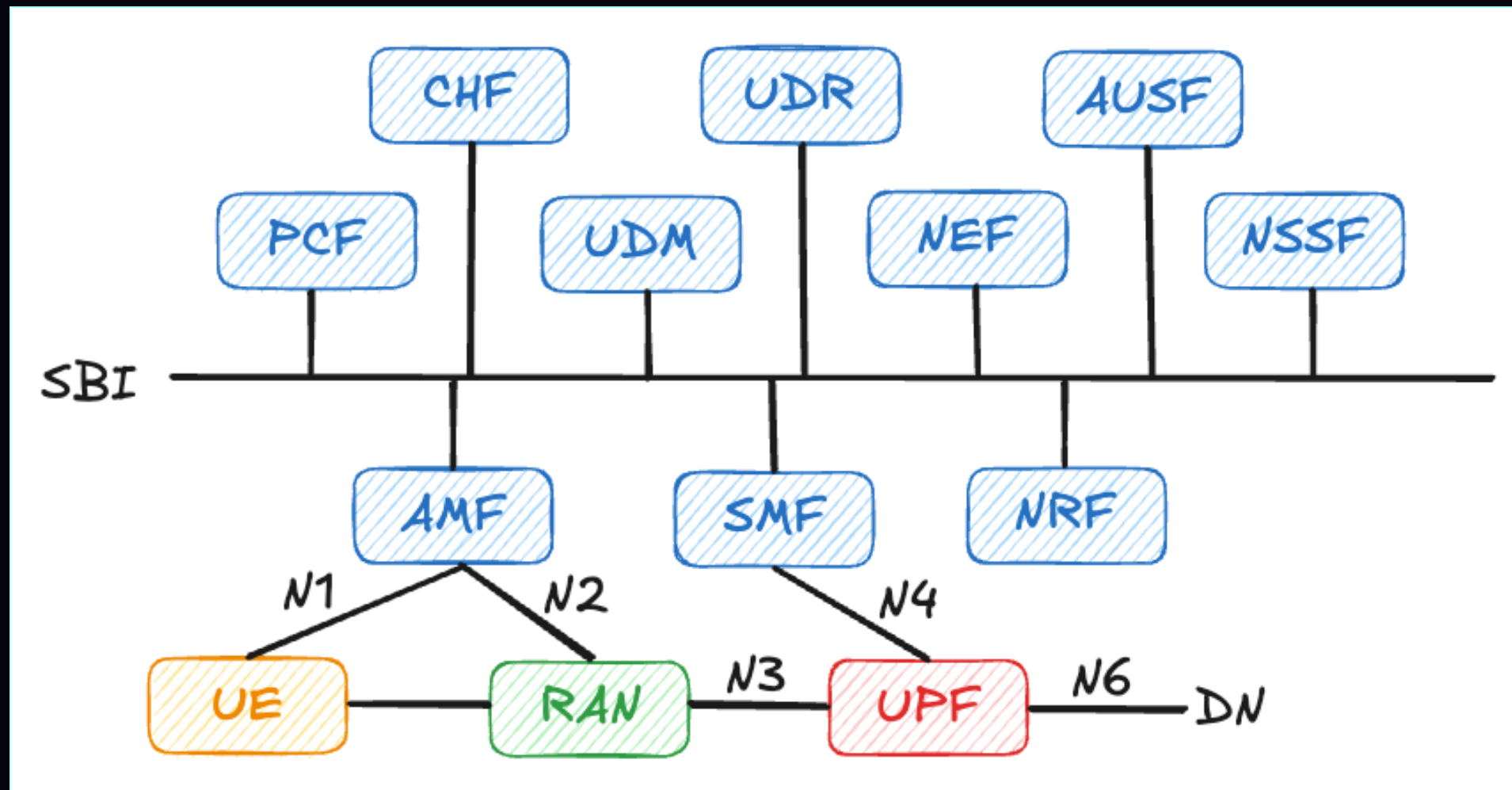
不可信任

TNGF

可信任

BSF、SCP 是原文沒有、但 free5GC 已經實作的 NF。

➤ 大家都掛在 SBI 上



控制面 NF 全在 SBI 上

彼此用 HTTP/2 互叫

只有 UPF 例外 (N4)

N3IWF / TNGF 走 N2 / N3

\$ PART 01

SBA 回顧

Service-Based Architecture：讓不同廠商的 NF 用同一種方式對話

／> 生產者與消費者

Producer

生產者 · 提供服務

把自己的能力包成服務

透過 SBI 對外公開

例：SMF 提供 nsmf-pdusession

Consumer

消費者 · 使用服務

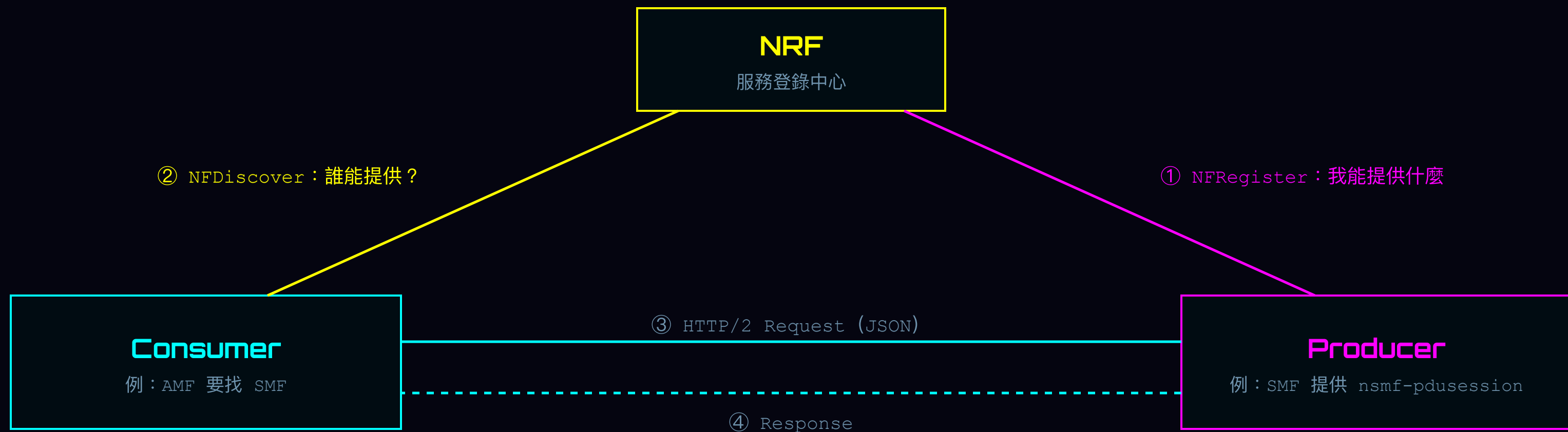
需要時呼叫別人的服務

先問 NRF 誰能提供

例：AMF 呼叫 SMF

同一個 NF 可以同時是生產者與消費者：SMF 對 AMF 是生產者，對 PCF 是消費者。

➤ 一次服務呼叫的四步



➤ SBI 用什麼協定？

5G SBI

TS 29.500 / 29.501

HTTP/2 + JSON (RESTful)

TLS 保護、OAuth 2.0 授權

OpenAPI 定義每個服務

未來：QUIC 解 TCP 隊頭阻塞

4G EPC

點對點介面

Diameter (S6a、Gx、Gy)

GTP-C (S11、S5)

每條介面一種協定

新增元件 = 新增介面

學界也有人嘗試用 gRPC 實作 SBI (SBA-gRPC-5G，NetSoft 2019)。

> SBI 的 URI 長這樣

`http://127.0.0.2:8000`

apiRoot (NF 位址)

`/nsmf-pdusession`

服務名稱

`/v1`

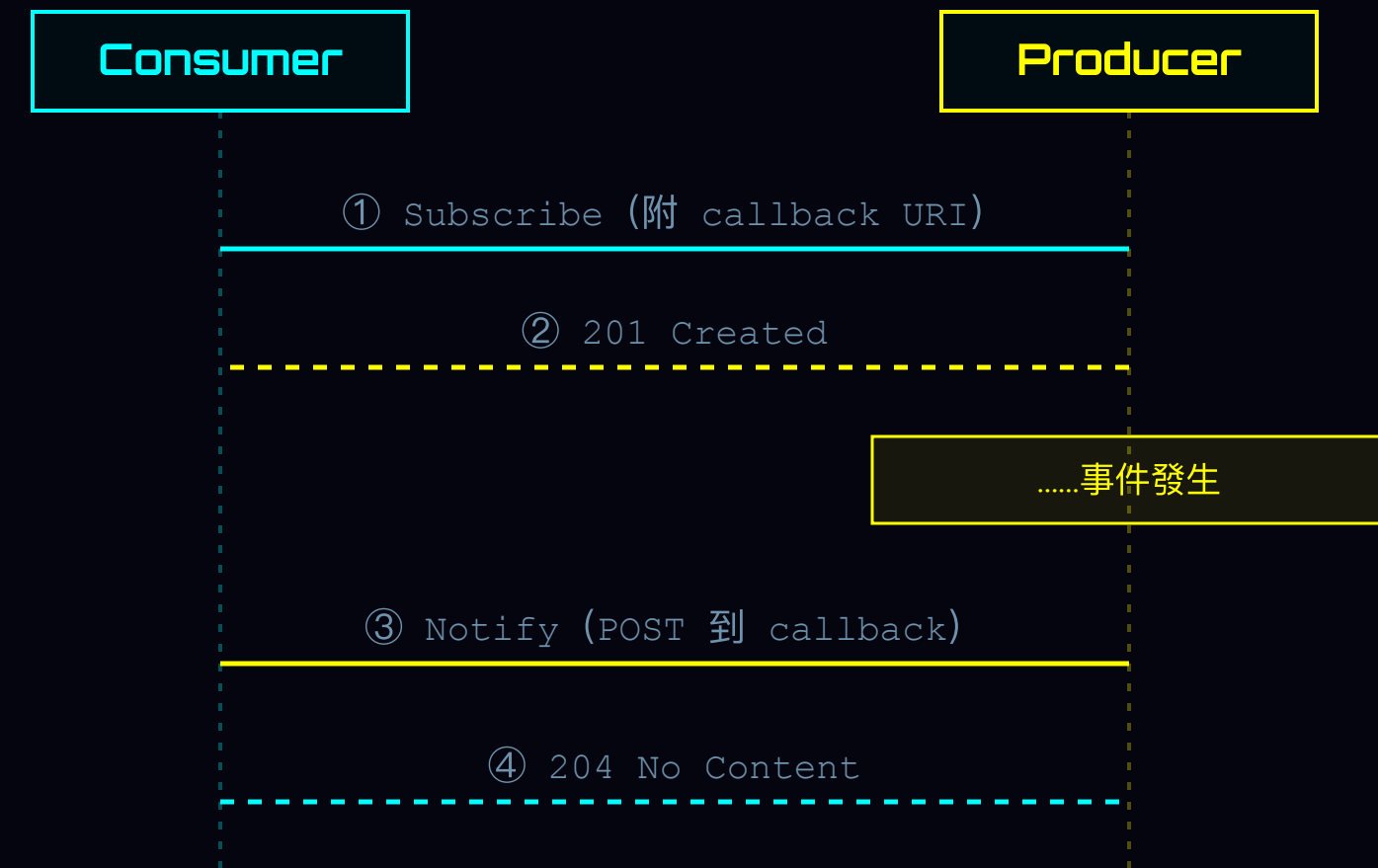
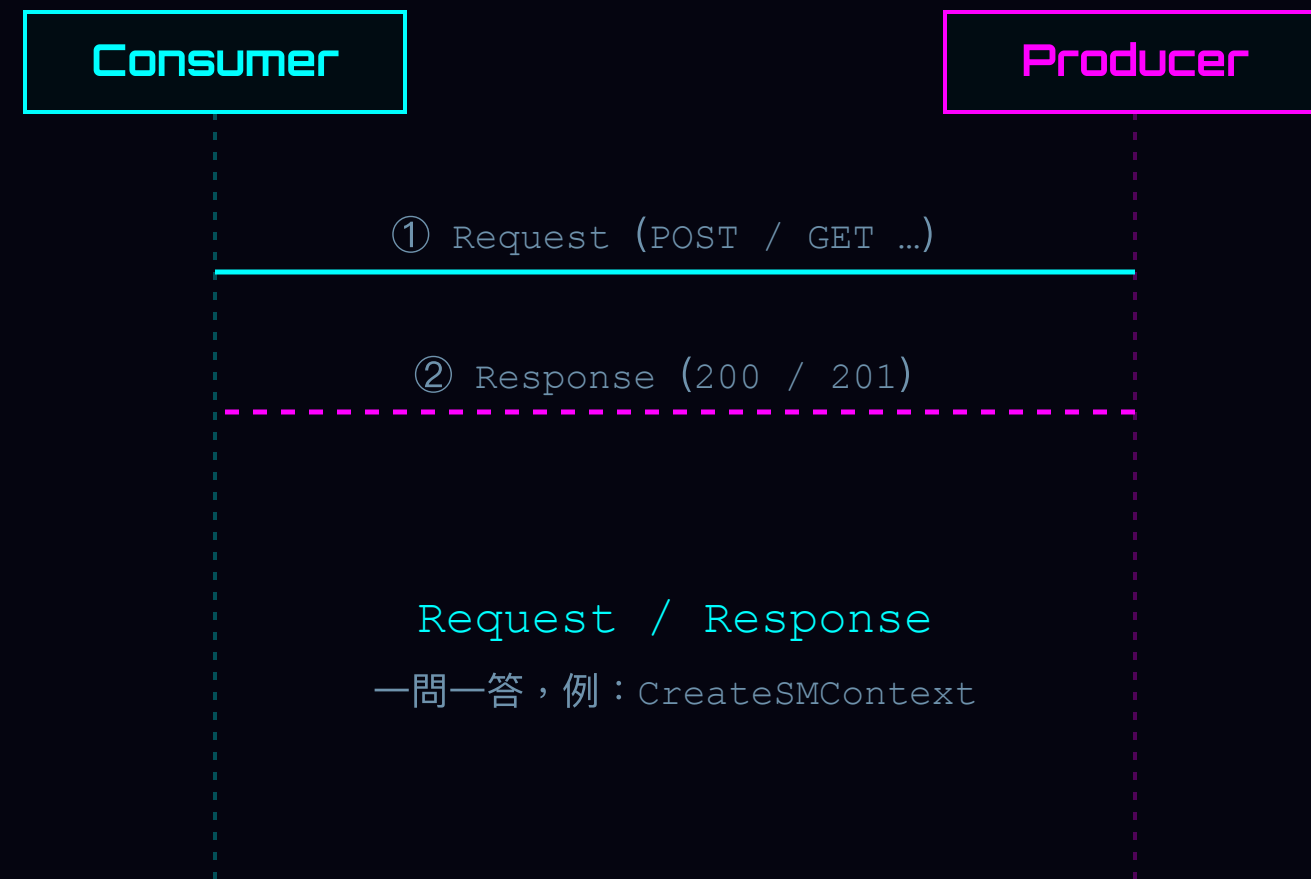
版本

`/sm-contexts`

資源

POST	<code>/nsmf-pdusession/v1/sm-contexts</code>	# 建立 SM Context
POST	<code>/nsmf-pdusession/v1/sm-contexts/{ref}/modify</code>	# 更新
GET	<code>/nudm-sdm/v2/{supi}/am-data</code>	# 讀訂閱資料

/> 兩種互動模式



Subscribe / Notify 讓 NF 不必一直輪詢；例如 PCF 訂閱 UDR 的資料變更。

/> 服務命名規則

NF	服務 (規格名稱)	URI 前綴
NRF	Nnrf_NFManagement / NFDiscovery	/nnrf-nfm、/nnrf-disc
AUSF	Nausf_UEAuthentication	/nausf-auth
UDM	Nudm_SDM / UECM / UEAU	/nudm-sdm、/nudm-uecm、/nudm-ueau
PCF	Npcf_SMPolicyControl	/npcf-smpolicycontrol
BSF	Nbsf_Management	/nbsf-management
CHF	Nchf_ConvergedCharging	/nchf-convergedcharging
NSSF	Nnssf_NSSelection	/nnssf-nsselection

規則：N + 小寫 NF 名稱 + 服務；看到 URI 前綴就知道是打給哪個 NF。

\$ PART 02

NRF

NF Repository Function : 5GC 的服務登錄中心與目錄服務

/> NRF 做什麼？

01

註冊管理

接收並維護 NF Profile

02

發現服務

依條件回傳合適的生產者

03

狀態監控

靠 Heartbeat 掌握存活

04

負載均衡

同類型多實例可分流

05

服務授權

誰可以呼叫誰

06

去註冊

NF 下線時移除

07

通知服務

NF 狀態變化通知訂閱者

08

存取令牌

OAuth 2.0 Access Token

NRF 沒有 4G 對應元件，是 5G 才有的全新設計。

➤ NRF 的三個服務

NFManagement

/nnrf-nfm

NFRegister (PUT)

NFUpdate (PATCH, Heartbeat)

NFDeregister (DELETE)

NFStatusSubscribe / Notify

NFDiscovery

/nnrf-disc

依 NF 類型查詢

可加 DNN、S-NSSAI 等條件

回傳 NF Profile 清單

AccessToken

/oauth2/token

OAuth 2.0 Client Credentials

簽發 JWT

標準中為選用

➤ NF PROFILE : NF 的自我介紹

```
{  
  "nfInstanceId": "b1c2...",  
  "nfType": "SMF",  
  "nfStatus": "REGISTERED",  
  "ipv4Addresses": ["127.0.0.2"],  
  "sNssais": [{ "sst": 1, "sd": "010203" }],  
  "nfServices": [{  
    "serviceName": "nsmf-pdusession", ... }],  
  "smfInfo": { "sNssaiSmfInfoList": ... },  
  "heartBeatTimer": 10  
}
```

我是誰：ID、類型

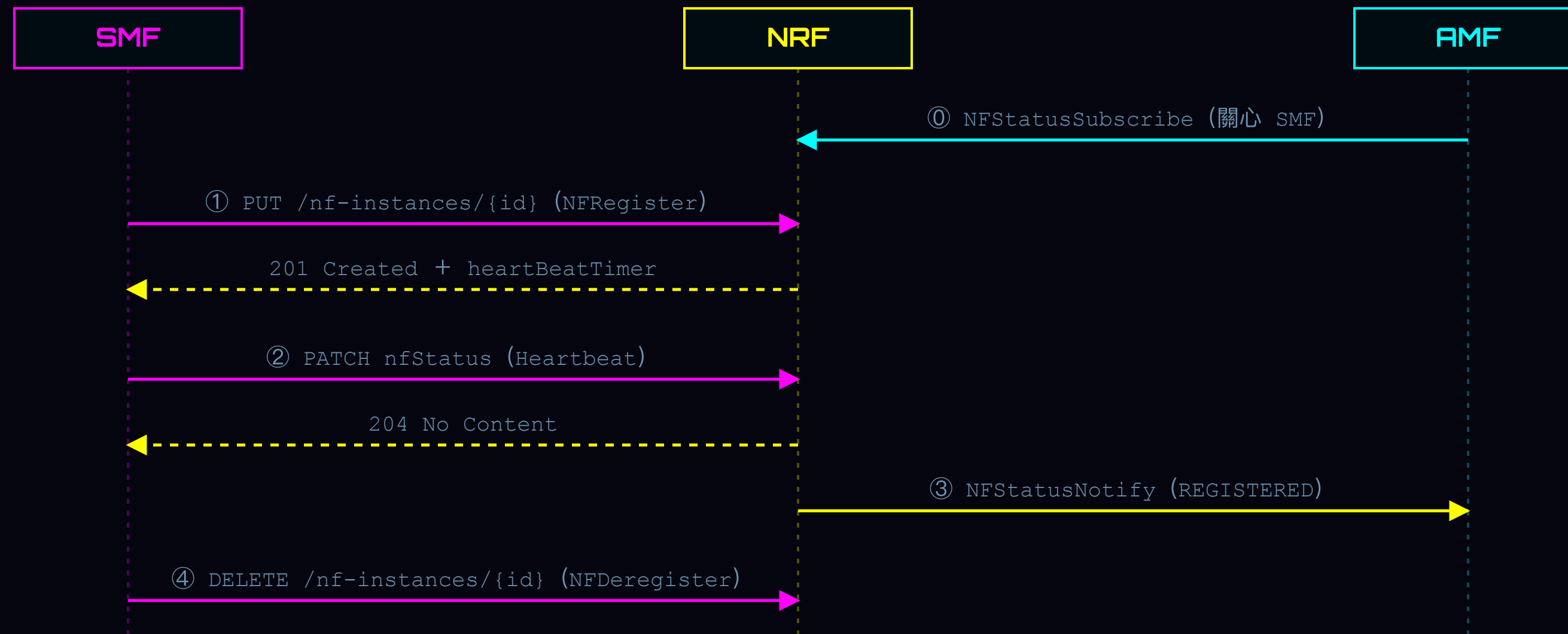
在哪裡：IP、FQDN

能做什麼：服務清單

服務誰：切片、DNN

多久報到一次

/> 註冊、心跳、通知、下線



DISCOVERY 查詢

```
GET /nnrf-disc/v1/nf-instances
    ?target-nf-type=SMF
    &requester-nf-type=AMF
    &service-names=nsmf-pdusession
    &dnn=internet
    &snssais=[{"sst":1,"sd":"010203"}]
```

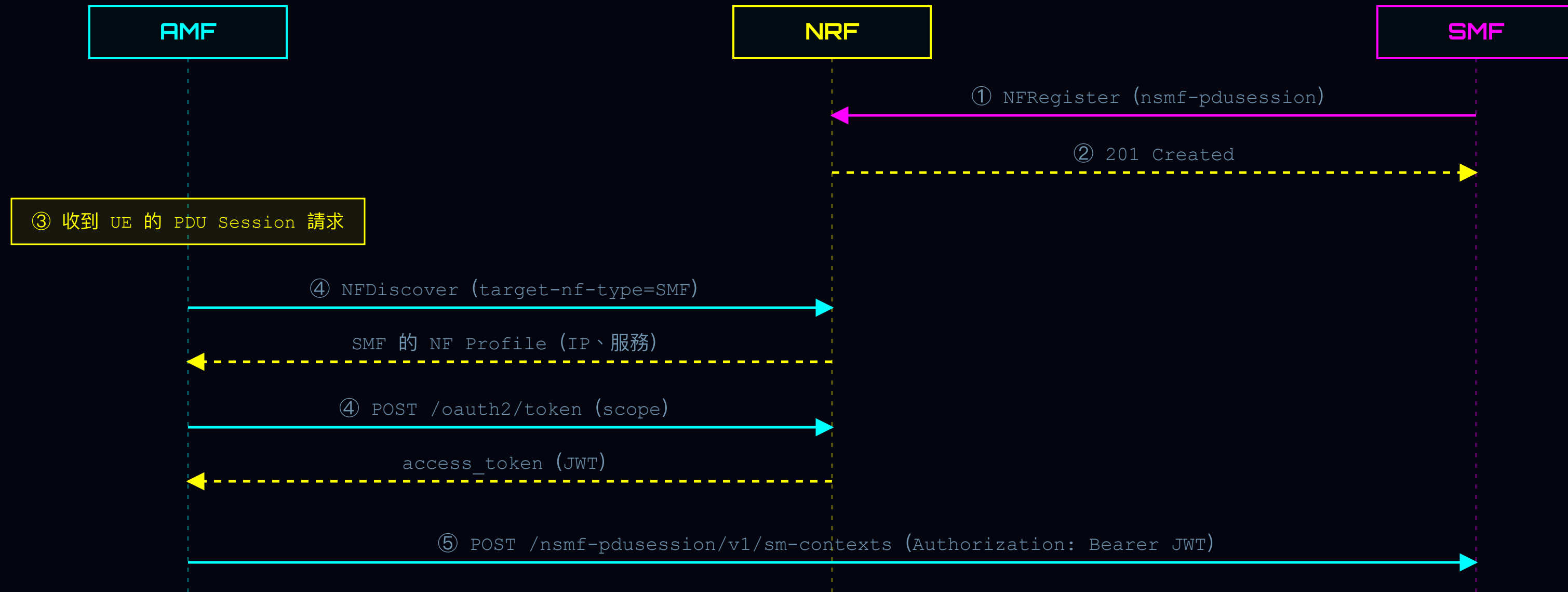
target / requester 必填

其餘條件用來篩選

回傳符合的 NF Profile

Consumer 自己挑一個

➤ AMF 怎麼找到 SMF ?



➤ ACCESS TOKEN 裡有什麼？

Header

alg: RS256

typ: JWT

Payload

iss: NRF 的 ID

sub: AMF 的 Instance ID

aud: SMF

scope: nsmf-pdusession

exp: 到期時間

Signature

NRF 用私鑰簽章

SMF 用 nrf.pem 驗證

SMF 不必回頭問 NRF：驗簽章、看 scope 和 exp，就能決定要不要服務這個請求。

➤ FREE5GC 的 NRF

```
# config/nrfcfg.yaml
MongoDBUrl: mongodb://127.0.0.1:27017
sbi:
  registerIPv4: 127.0.0.10
  port: 8000
  oauth: true          # 開啟 Token 驗證
serviceNameList:
  - nnrf-nfm
  - nnrf-disc

# 其他 NF 的設定檔
nrfUri: http://127.0.0.10:8000
nrfCertPem: cert/nrf.pem
```

NF Profile 存在 MongoDB

UPF 之後第一個啟動

每個 NF 都要知道 nrfUri

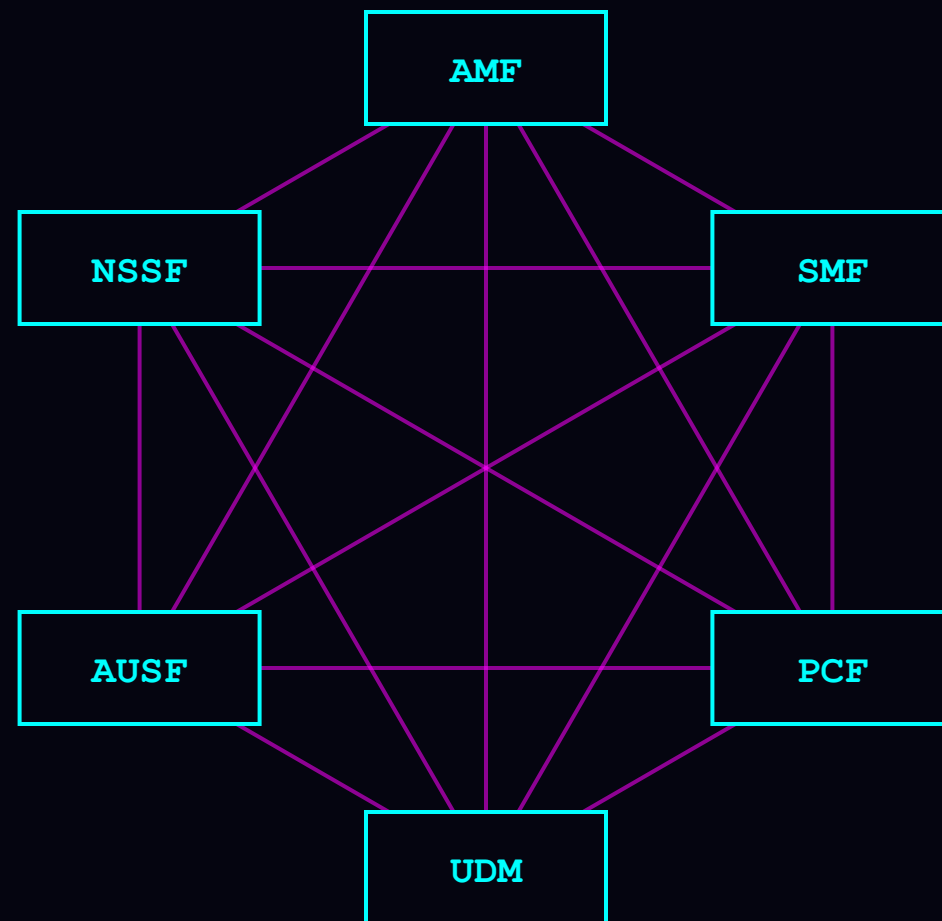
nrf.pem 用來驗 JWT

\$ PART 03



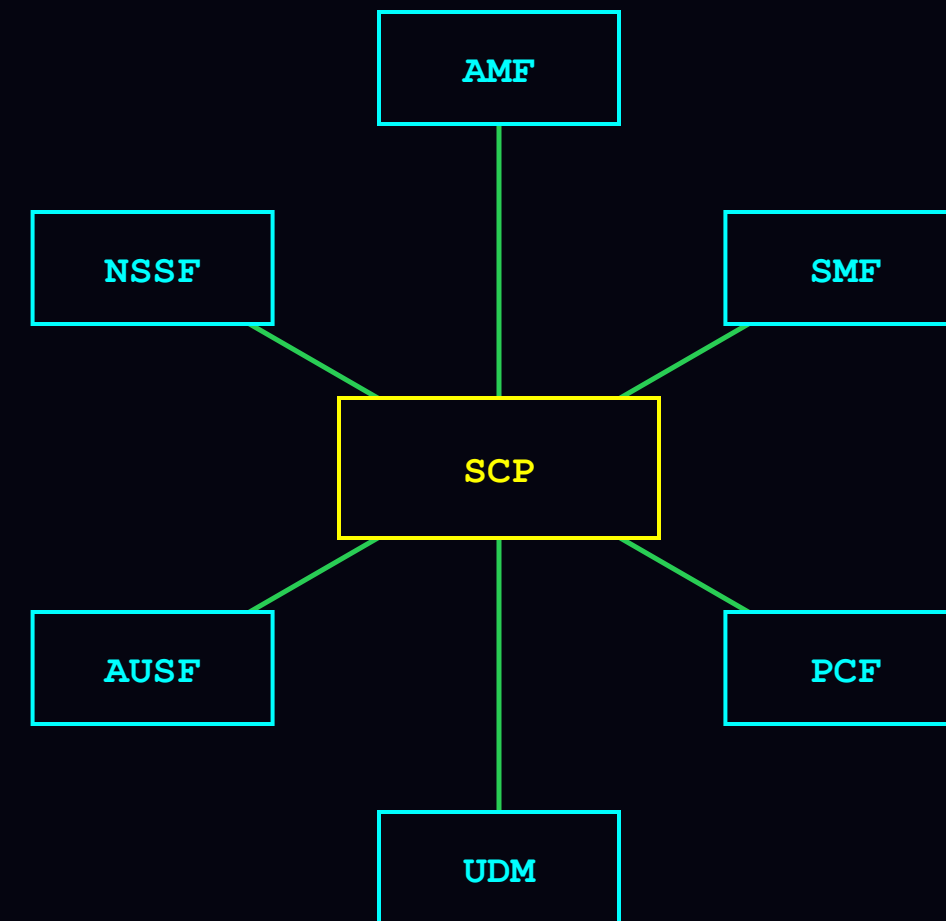
Service Communication Proxy：讓 NF 之間的訊息有一個集中轉送的代理（原文未提、free5GC 已實作）

➤ 為什麼需要 SCP ?



Direct : 6 個 NF → 15 條連線

N 個 NF $\approx N(N-1)/2$, 每條都要 discovery、TLS、重試



Indirect : 大家只連 SCP

路由、負載平衡、重試集中在 SCP

➤ SCP 做什麼？

01

間接通訊

Consumer 的請求先送到 SCP，再轉給 Producer

02

代理 Discovery

Consumer 只給條件，由 SCP 去問 NRF 並挑選

03

負載平衡與重試

Producer 掛了，SCP 換一個實例重送

04

集中觀測與管控

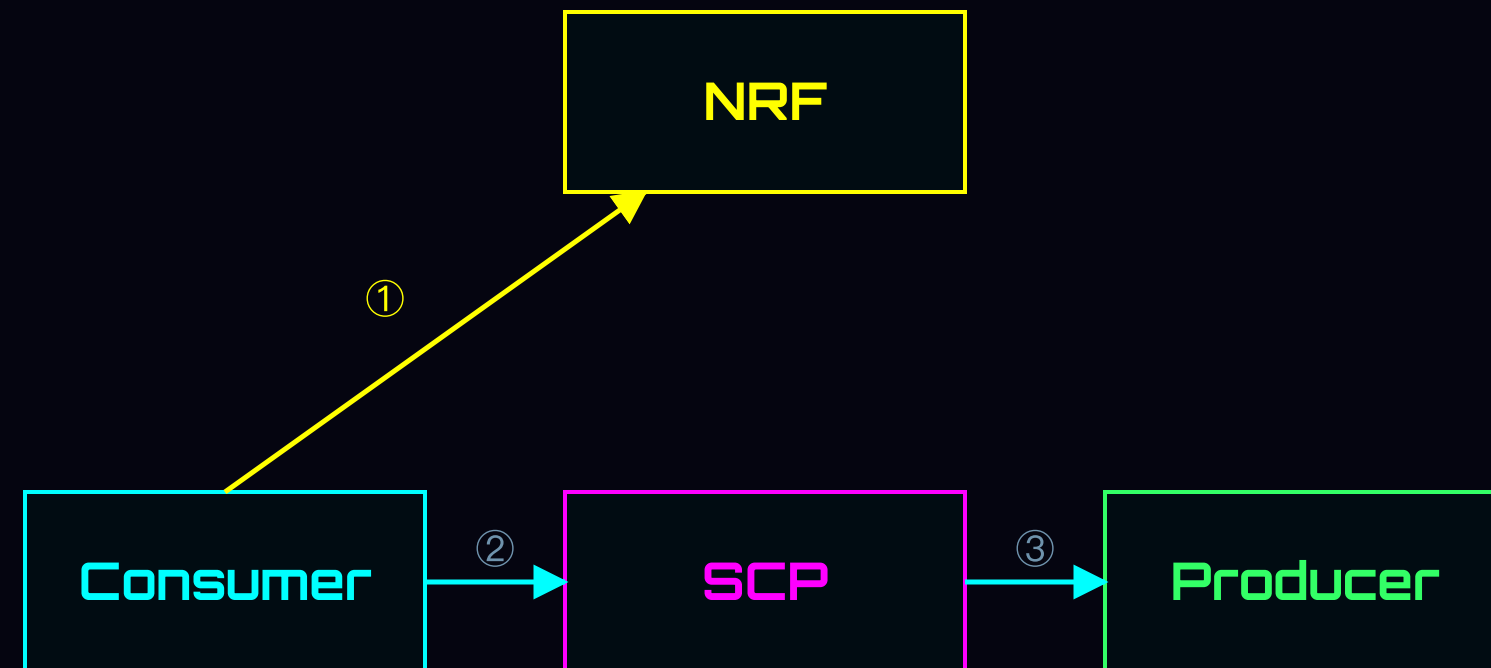
流量統計、過載控制、異常偵測集中在一處

SCP 在 Rel-16 引入；跨電信商的邊界代理是另一個 NF：SEPP。

➤ 四種溝通模型 (TS 23.501 ANNEX E)

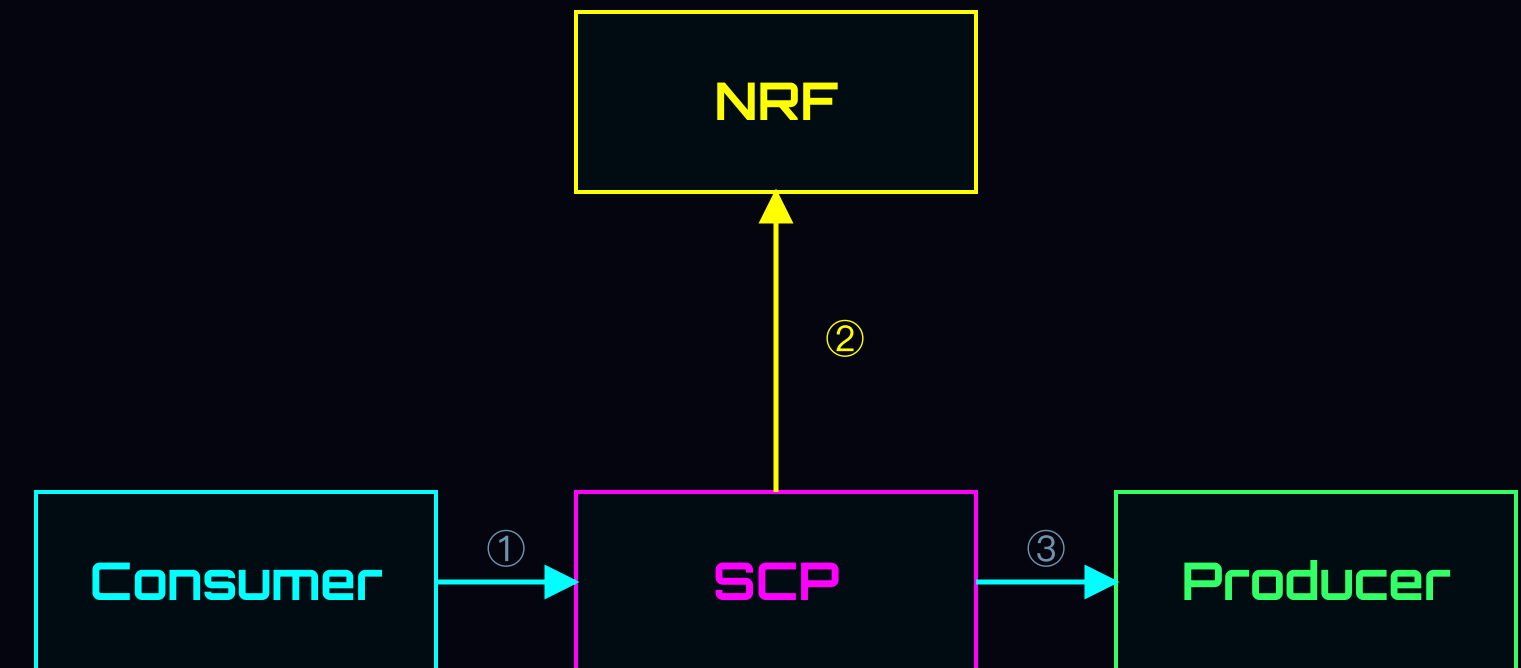
MODEL	直接 / 間接	誰做 DISCOVERY	說明
A	直接	不做 (寫死設定)	最早期、最簡單
B	直接	Consumer 問 NRF	目前 free5GC 預設
C	間接 (經 SCP)	Consumer 問 NRF	選好目標，交給 SCP 送
D	間接 (經 SCP)	SCP 代為查詢	Delegated Discovery

➤ MODEL C 與 MODEL D



Model C：自己找、SCP 轉送

- ① Consumer 自己 discovery，選定 Producer
- ②③ 請求經 SCP 送到指定的 Producer



Model D：連找都交給 SCP

- ① 只帶「條件」給 SCP (Delegated Discovery)
- ②③ SCP 代為 discovery，再轉送

／> 經過 SCP 時多帶的 HEADER

HTTP HEADER (TS 29.500)	用途
3gpp-Sbi-Target-apiRoot	Model C：告訴 SCP 真正的目標 Producer
3gpp-Sbi-Discovery-*	Model D：交給 SCP 的查詢條件（例：target-nf-type）
3gpp-Sbi-Routing-Binding	後續請求要綁回同一個實例
3gpp-Sbi-Callback	標示這是 Notify 之類的回呼訊息

Body 不變，路由資訊放在 Header：SCP 不需要看懂每一種服務的 JSON。

➤ FREE5GC 的 SCP

```
# config/scpcfg.yaml
sbi:
  registerIPv4: 127.0.0.6
  port: 8000
serviceList:
  - serviceName: nausf-auth
  - serviceName: nudm-ueau
  - serviceName: nudm-sdm
  - serviceName: nudr-dr
ausfUri: http://127.0.0.9:8000
udmUri:  http://127.0.0.3:8000
udrUri:  http://127.0.0.4:8000
... (AMF、SMF、PCF...的真實位址)
```

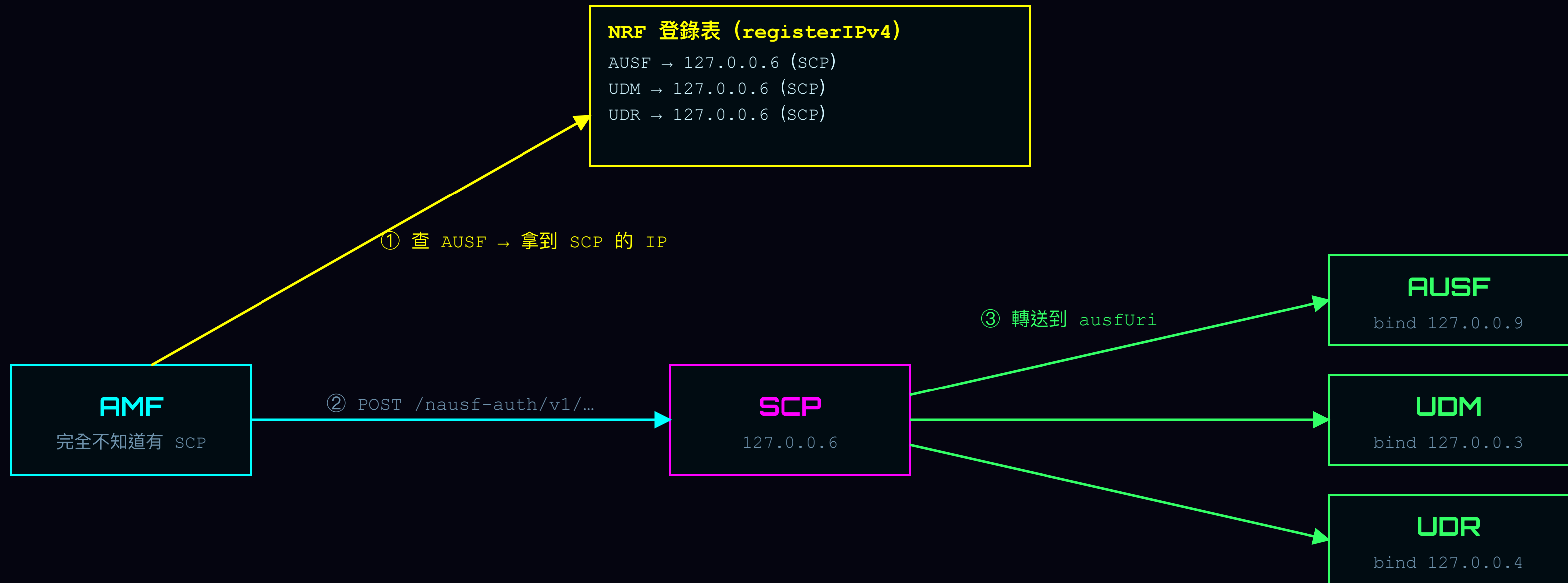
預設不啟動

```
./run.sh -scp
```

目前聚焦認證路徑

設定裡寫死真實位址

➤ CONSUMER 怎麼「不知不覺」經過 SCP?



Producer 對 NRF 宣告 SCP 的位址、自己仍綁原本的 IP → AUSF→UDM、UDM→UDR 也都會經過 SCP

➤ SCP 收到請求之後

```
// 1. 有實作的路由：解析後重新送出
/nausf-auth/v1/ue-authentications           → AUSF
/nausf-auth/v1/.../5g-aka-confirmation      → AUSF
/nudm-ueau/v1/.../generate-auth-data        → UDM
/nudr-dr/v1/.../authentication-subscription → UDR

// 2. 其他路徑：NonSupportAPI()
nf := regexp("^/n([a-z]+)") // /nsmf-... → "smf"
uri := ctx.URIForNF("SMF")  // 查設定檔
http.Do(原樣轉送 method / header / body)
```

認證三服務：逐一處理

其他：看 URI 前綴轉送

轉送時自己拿 Token

➤ FREE5GC SCP 與 3GPP SCP

3GPP 的 SCP

TS 23.501 / 29.500

Model C / D 間接通訊

靠 3gpp-Sbi-* Header 路由

Consumer 知道 SCP 存在

可代為 Discovery、重選

free5GC 的 SCP

透明代理

Producer 宣告 SCP 位址

Consumer 完全不用改

目標寫在 SCP 設定檔

適合觀察、偵測認證流量

原始碼裡的 log 叫 DetectorLog：這個 SCP 也被拿來做異常偵測的實驗平台。

\$ PART 04



Authentication Server Function：專門負責核對身分與密碼的後端服務

> AUSF 的位置



4G：MME ↔ HSS (AuC) → 5G：AMF ↔ AUSF ↔ UDM，認證結果由 Home 網路的 AUSF 拍板

AMF 把 UE 帶到櫃檯，AUSF 核對身分，UDM 保管鑰匙。

/> AUSF 做什麼？

01

用戶認證

執行 5G-AKA 程序

02

金鑰管理

產生並保管 KAUSF、推導 KSEAF

03

認證向量

把 HE AV 轉成 SE AV 給 AMF

04

EAP 支援

EAP-AKA' 認證方法

05

狀態管理

記錄認證結果與 Context

06

漫遊認證

漫遊時由 Home AUSF 認證

➤ 5G 的用戶識別碼

識別碼	是什麼	例子 / 特性
SUPI	永久身分 (≈ IMSI)	imsi-2089300000000001，不在空中明文傳
SUCI	加密後的 SUPI	每次都不同，防追蹤
5G-GUTI	暫時身分	AMF 分配，註冊後用它
GPSI	對外身分 (≈ MSISDN)	電話號碼，給外部應用用

➤ SUCI : 把 SUPI 藏起來

SUPI Type	Home Network	Routing Ind.	Scheme	Key ID	Scheme Output
IMSI / NAI	MCC + MNC	選 UDM 用	Null / A / B	哪把公鑰	加密後的 MSIN

UE : 用 Home 網路的公鑰 (ECIES) 加密 MSIN

UDM 的 SIDF : 用私鑰解回 SUPI

Scheme 為 Null 時等於不加密，free5GC 測試常用；Profile A / B 分別用 X25519 / secp256r1。

➤ 5G-AKA 要達成什麼？

01

互相認證

UE 用 AUTN 驗網路；網路用 RES* 驗 UE

02

金鑰協商

雙方各自算出同一把 KSEAF，不在空中傳

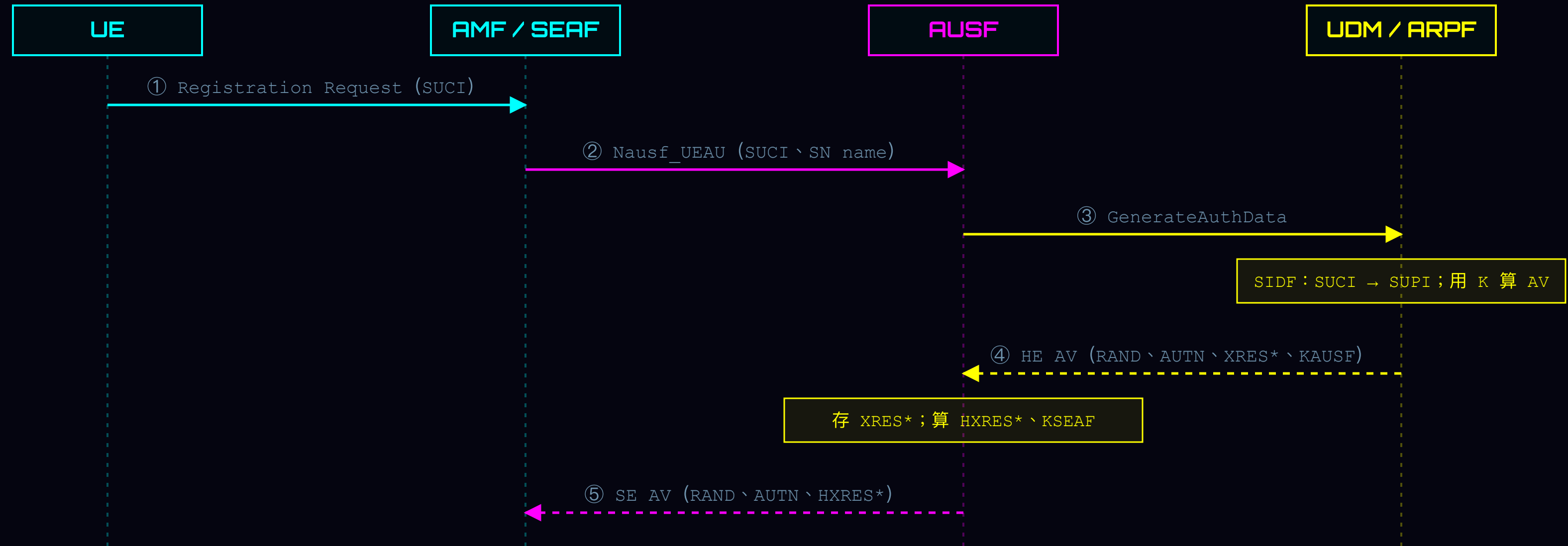
03

HOME 拍板

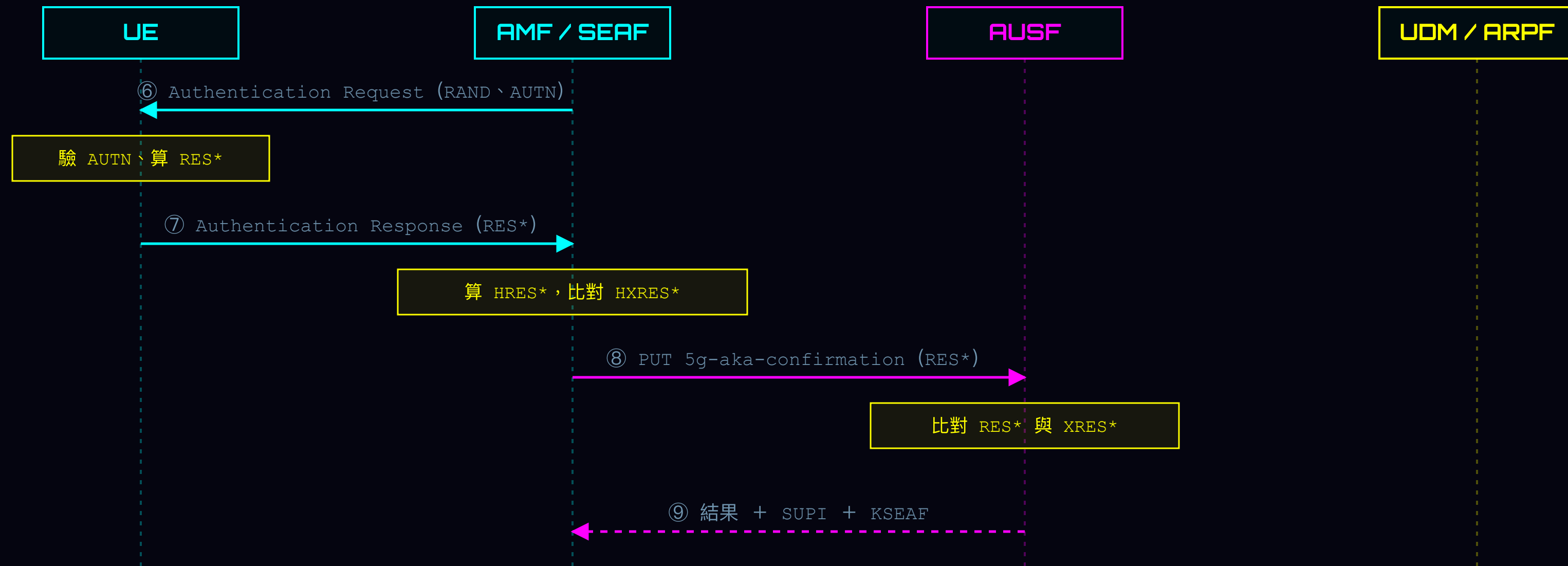
最終由 Home 的 AUSF 確認，不只信漫遊地

4G EPS-AKA 由 MME 比對就結束；5G 多了 AUSF 的確認，Home 網路握有最後決定權。

➤ 5G-AKA (上) : 準備向量



➤ 5G-AKA (下)：挑戰與確認



／> 兩種認證向量

5G HE AV

Home Environment · UDM → AUSF

RAND：隨機挑戰

AUTN：網路的證明

XRES*：預期答案

KAUSF：AUSF 的金鑰

5G SE AV

Serving Environment · AUSF → AMF

RAND：原封不動

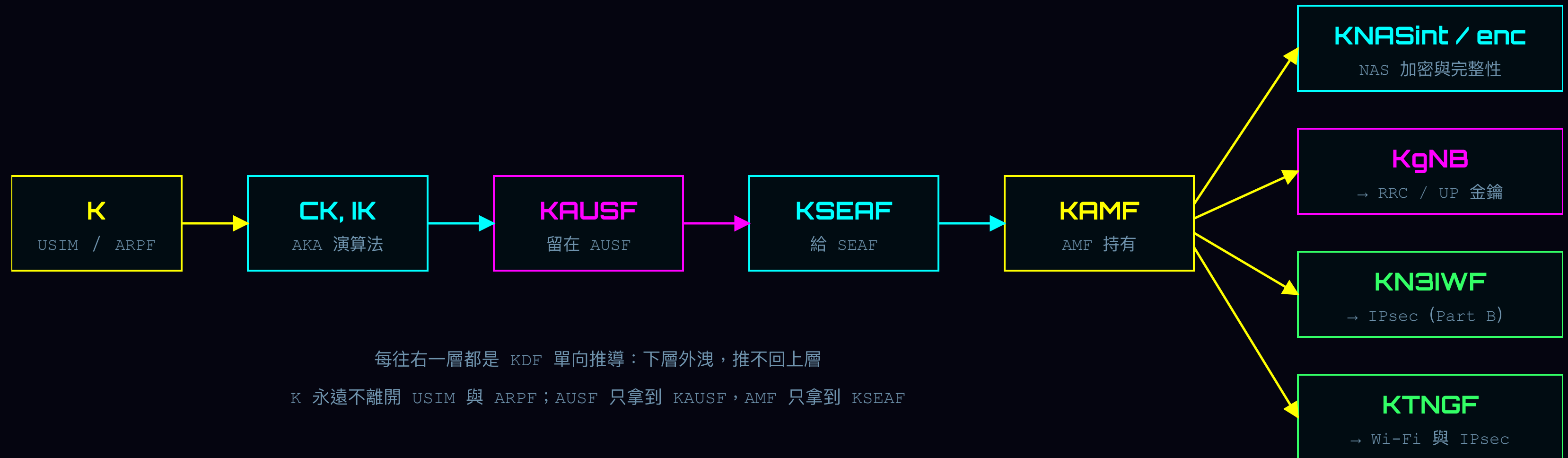
AUTN：原封不動

HXRES*：答案的雜湊

(沒有 KAUSF)

AMF 只拿到答案的雜湊，能先擋掉錯誤回應，但真正的答案只有 AUSF 知道。

／> 金鑰階層



/> 5G-AKA 與 EAP-AKA'

比較	5G-AKA	EAP-AKA'
封裝方式	NAS 訊息直接帶	包在 EAP 封包裡
誰先比對	AMF 比 HRES*，AUSF 再比 RES*	AUSF 當 EAP Server 比對
KAUSF 來源	CK IK 推導	CK' IK' → EMSK
常見場景	3GPP 接入	非 3GPP、企業 / 專網
free5GC API	.../5g-aka-confirmation	.../eap-session

➤ FREE5GC 的認證 API 路徑

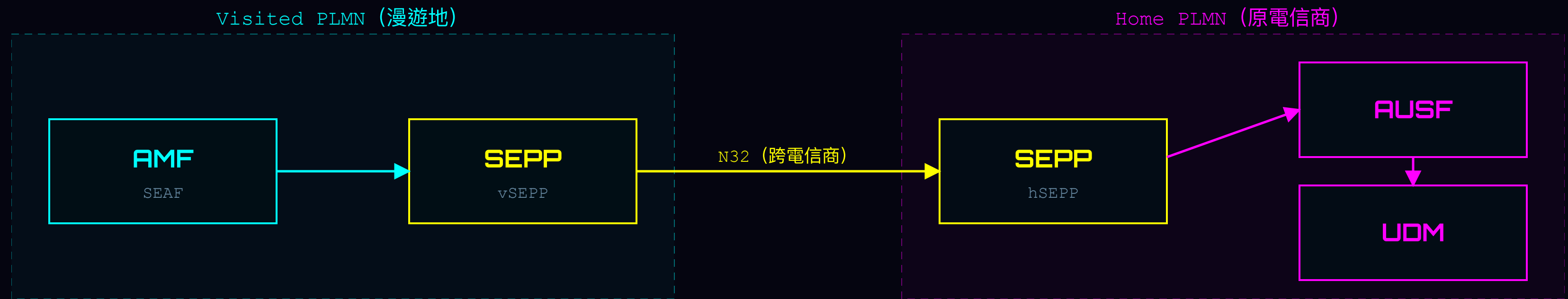
```
# AMF → AUSF
POST /nausf-auth/v1/ue-authentications # 帶 SUCI、SN name
PUT /nausf-auth/v1/ue-authentications/{ctxId}/5g-aka-confirmation
POST /nausf-auth/v1/ue-authentications/{ctxId}/eap-session

# AUSF → UDM
POST /nudm-ueau/v1/{suci}/security-information/generate-auth-data

# UDM → UDR
GET /nudr-dr/v1/subscription-data/{supi}/authentication-data/authentication-subscription
PATCH ... (更新 SQN，防重放)
```

K、OPc、SQN 存在 authenticationSubscription，就是在 Webconsole 新增 UE 時填的那幾格。

／> 漫遊認證



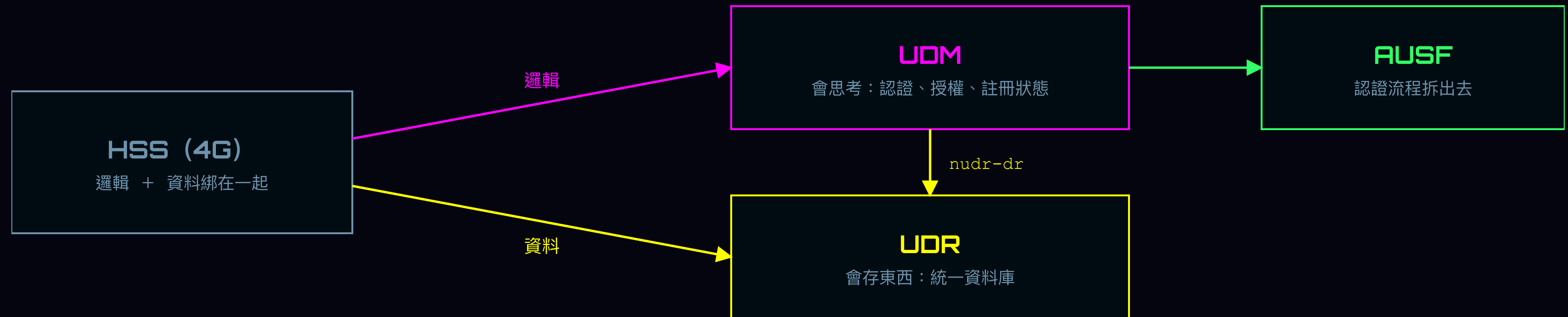
漫遊時 AMF 在別人家，但「你是誰」仍由 Home 的 AUSF / UDM 決定

\$ PART 05

UDM / UDR

一個會思考、一個會存東西 -- 再加上 free5GC 的 Webconsole

➤ 4G 的 HSS 被拆開了



資料與邏輯分離：UDM 可以水平擴充，資料統一放在 UDR。

/> UDM 做什麼？

01

身分管理

SUPI、GPSI

02

訂閱資料

服務權限、QoS

03

認證資料

K、HE AV 產生

04

接取與移動

註冊狀態、服務的 AMF

05

會話資料

DNN、SMF 選擇

06

隱私保護

SIDF 解 SUCI

07

服務授權

誰能讀哪些資料

08

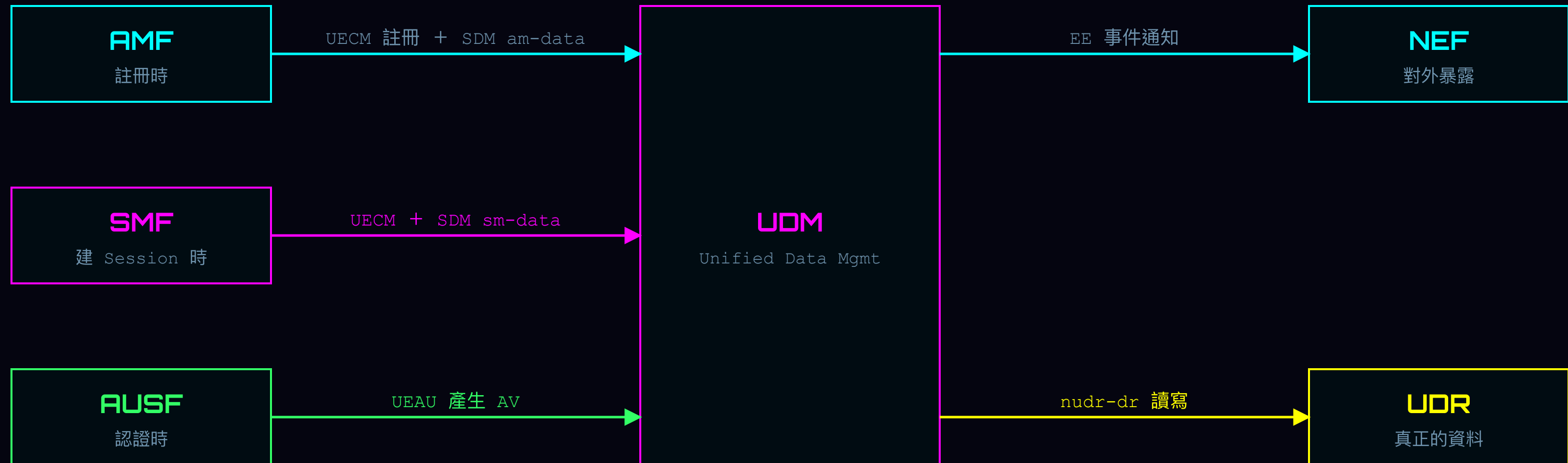
事件暴露

狀態變化通知 NEF

/> UDM 的服務

服務	做什麼	誰呼叫・何時
Nudm_UEAU	產生認證向量	AUSF・認證時
Nudm_UECM	登記「誰在服務這個 UE」	AMF / SMF・註冊、建 Session
Nudm_SDM	提供訂閱資料 (am / sm / smf-select)	AMF / SMF・需要資料時
Nudm_EE	事件訂閱與通知	NEF・對外暴露
Nudm_PP	外部設定參數	NEF・例如預期 UE 行為

➤ 誰會來找 UDM ?



➤ UDM 與 UDR 別搞混

UDM

會思考的服務

提供 API 與 5GC 邏輯

誰能用、怎麼驗證

允許哪些切片 / DNN

參與訊號流程

UDR

會存東西的資料庫

統一儲存各 NF 的資料

包含 UDM 的資料

不做決策

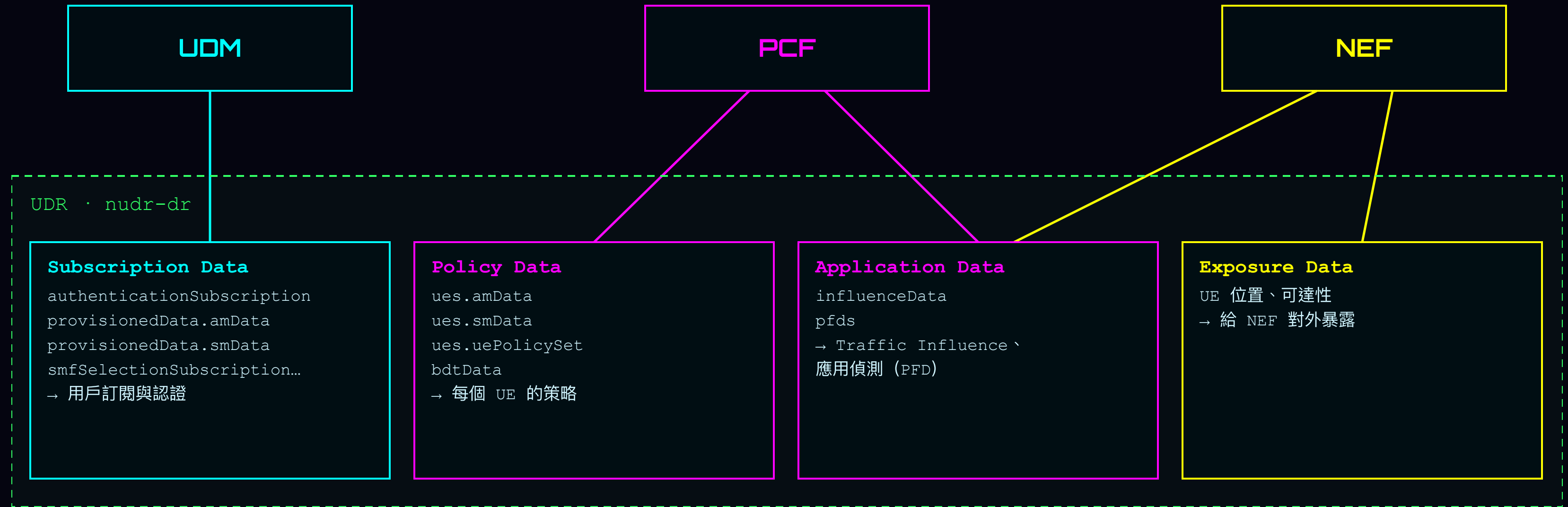
不直接參與訊號流程

/> UDR 做什麼？



UDR 用 GET、POST、PUT、PATCH、DELETE 操作資料；在某些部署中 UDSF 也會經由 UDR 存放非結構化資料。

➤ UDR 的四類資料



➤ FREE5GC 的 MONGODB COLLECTION

COLLECTION	內容	誰要用（怎麼拿）
<code>subscriptionData.authenticationData.authenticationSubscription</code>	K、OPc、SQN	UDM（經 UDR）
<code>subscriptionData.provisionedData.amData</code>	切片、AMBR	AMF（經 UDM → UDR）
<code>subscriptionData.provisionedData.smData</code>	DNN、5QI、Session AMBR	SMF（經 UDM → UDR）
<code>policyData.ues.smData</code>	SM Policy Data	PCF（經 UDR）
<code>policyData.ues.flowRule</code>	Flow Rule	PCF（直接讀 DB）
<code>policyData.ues.qosFlow</code>	QoS Flow	PCF（直接讀 DB）
<code>applicationData.influenceData</code>	Traffic Influence	PCF（經 UDR）

UDM 不連 MongoDB，一律經 UDR；PCF 是例外：Webconsole 設的 Flow Rule、QoS、計費直接讀 DB（實作捷徑，非標準作法）。

➤ NUDR-DR 的路徑

訂閱資料 (UDM 用)

GET /nudr-dr/v1/subscription-data/{ueId}/{servingPlmnId}/provisioned-data/am-data

GET /nudr-dr/v1/subscription-data/{ueId}/{servingPlmnId}/provisioned-data/sm-data

策略資料 (PCF 用)

GET /nudr-dr/v1/policy-data/ues/{ueId}/sm-data

應用資料 (NEF / AF 用, W6 的 Traffic Influence)

PUT /nudr-dr/v1/application-data/influenceData/{influenceId}

路徑第一層就分出四類資料：subscription-data、policy-data、application-data、exposure-data。

➤ WEB CONSOLE：輕量版 OAM

資料管理

直接操作 MongoDB

新增 / 刪除 / 修改 UE

切片、DNN、QoS 設定

Flow Rule 與計費設定

狀態與報表

核心網運作時

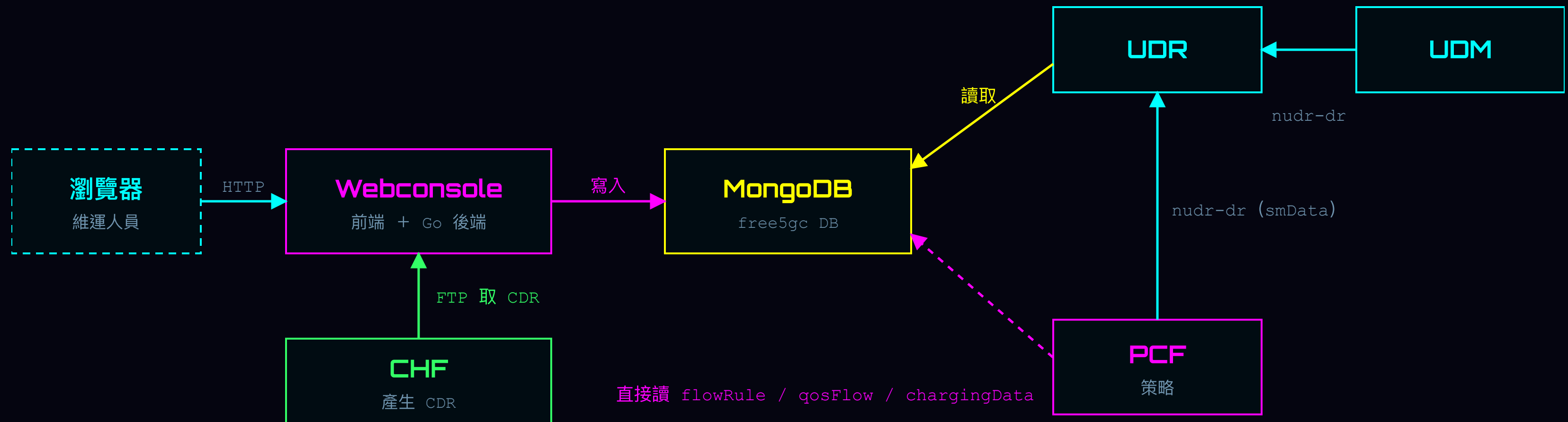
查看已註冊的 UE

透過 FTP 向 CHF 取 CDR

匯出使用量與計費報告

3GPP 要求要有 OAM 介面；free5GC 沒做完整 OAM，而是提供這個圖形化工具。欄位細節在第 11 章。

/> WEB CONSOLE 的架構



/> 新增一個 UE 之後

1

Webconsole → MongoDB

寫入 authenticationSubscription、amData、smData、policyData ...

2

認證：AUSF → UDM → UDR

讀出 K、OPc、SQN，算認證向量

3

註冊：AMF → UDM → UDR

讀 amData：可用切片、AMBR

4

建 Session：SMF → UDM → UDR、PCF → UDR + DB

SMF 拿 DNN、5QI；PCF 經 UDR 拿 smData，Flow Rule、QoS 直接讀 MongoDB

\$ PART 06



Policy Control Function：決定頻寬、能不能進某個 DNN、用哪種計費

➤ PCF 管四種策略

N7 · SMF

會話管理策略

QoS、Gating、計費、流量偵測、路由 (PCC Rule)

N15 · AMF

接取管理策略

RAT / 頻率優先序、服務區域限制、位置追蹤

N5 · AF

策略授權

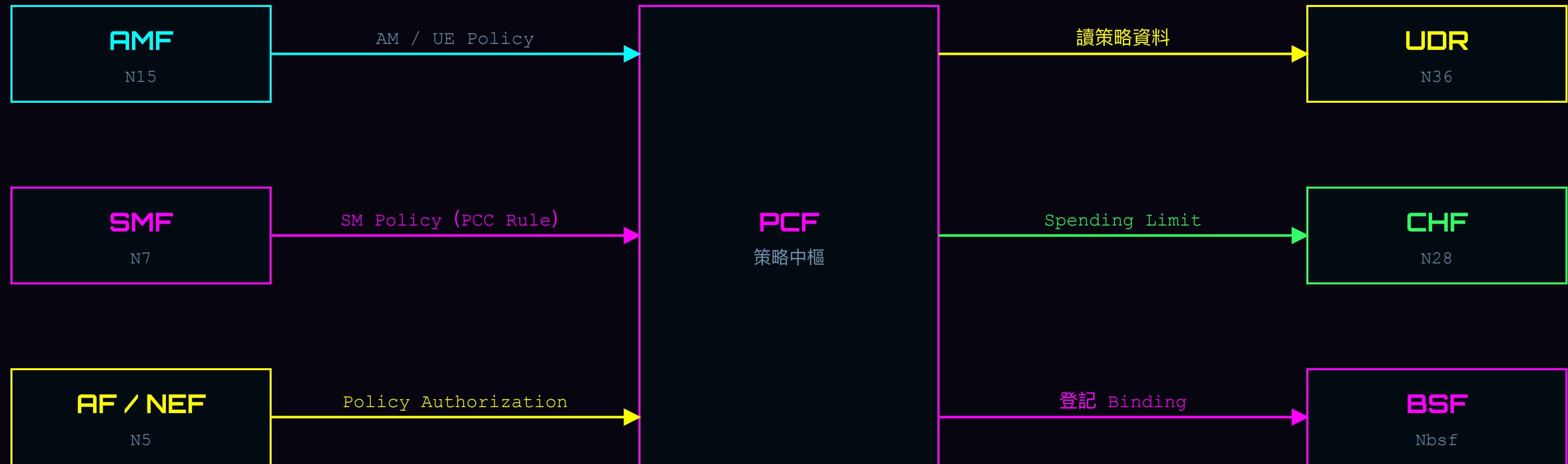
依應用要求動態建立策略，例如 IMS 語音

N15 · AMF → UE

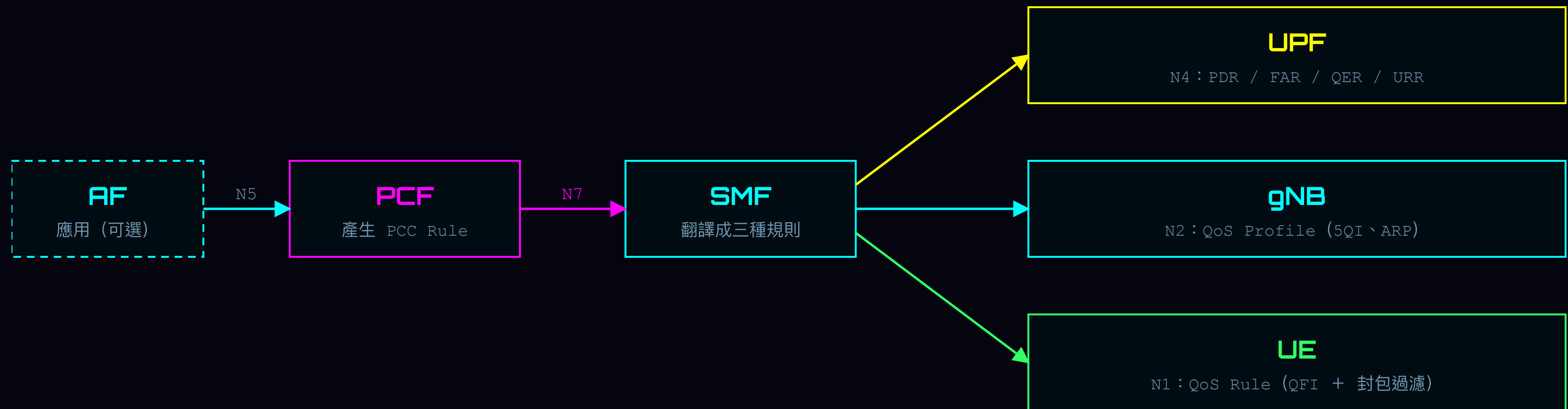
UE 策略

URSP：UE 自己決定哪個 App 走哪個 Session

➤ PCF 的介面



／> 會話管理策略：PCC RULE 怎麼落地



PCF 只說「要什麼」，SMF 把它翻成 UPF、gNB、UE 各自看得懂的規則（W6 的 PDR / FAR / QER / URR）。

➤ 接取管理策略 (N15)

RFSP

頻率優先序

RAT / Frequency Selection Priority，交給 RAN
決定 UE 優先待在哪

SAR

服務區域限制

UE 只能在允許的 TA 使用服務

LOC

位置追蹤

啟用定期回報，掌握 UE 目前位置

AMF 在註冊流程中建立 AM Policy Association，向 PCF 拿這些策略。

> UE 策略：URSP

優先序	TRAFFIC DESCRIPTOR (哪些流量)	ROUTE SELECTION (走哪條 SESSION)
1	App = 企業 VPN	S-NSSAI 1/010203、DNN = enterprise
2	目的地 = *.game.com	URLLC 切片、DNN = internet
3	目的地 = *.video.com	eMBB、偏好 Non-3GPP
255	Match-all	DNN = internet (預設)

URSP 經 AMF 以 NAS 送到 UE；UE 依規則把 App 的流量放進對應的 PDU Session。

➤ 策略授權 (N5) : VONR 例子

1

P-CSCF (AF) → PCF

通話要開始了：要一條語音 Flow (IP、Port、頻寬)

2

PCF 產生 PCC Rule

5QI = 1、GBR、對應的 SDF 過濾條件

3

PCF → SMF (UpdateNotify)

SMF 建立新的 QoS Flow

4

SMF → UPF / gNB / UE

PFCP、N2、N1 同時更新，語音有保證頻寬

➤ FREE5GC 的 PCF

SM Policy Data：經 UDR

Flow Rule、QoS：直接讀 MongoDB

訂閱 influenceData (W6 的 TI)

可選：向 BSF 登記 Binding

```
# config/pcfcfg.yaml (節錄)
sbi:
  registerIPv4: 127.0.0.7
serviceList:
  - serviceName: npcfc-am-policy-control
  - serviceName: npcfc-smpolicycontrol
  - serviceName: npcfc-policyauthorization
  - serviceName: npcfc-ue-policy-control
bsf:
  enable: true      # 預設就開；找不到 BSF 會 fallback
```

\$ PART 07

/> BSF

Binding Support Function：記住「這條 Session 是哪個 PCF 在管」（原文未提、free5GC 已實作）

／> 有很多 PCF 時，AF 該找誰？



AF 找錯 PCF，策略就套不到這條 Session 上。需要一本「Session ↔ PCF」的對照簿。

/> BSF 是什麼？

Binding

一筆對照資料

UE IP / MAC / SUPI / GPSI

DNN、S-NSSAI

→ 負責的 PCF 位址

Nbsf_Management

TS 29.521

Register：PCF 登記

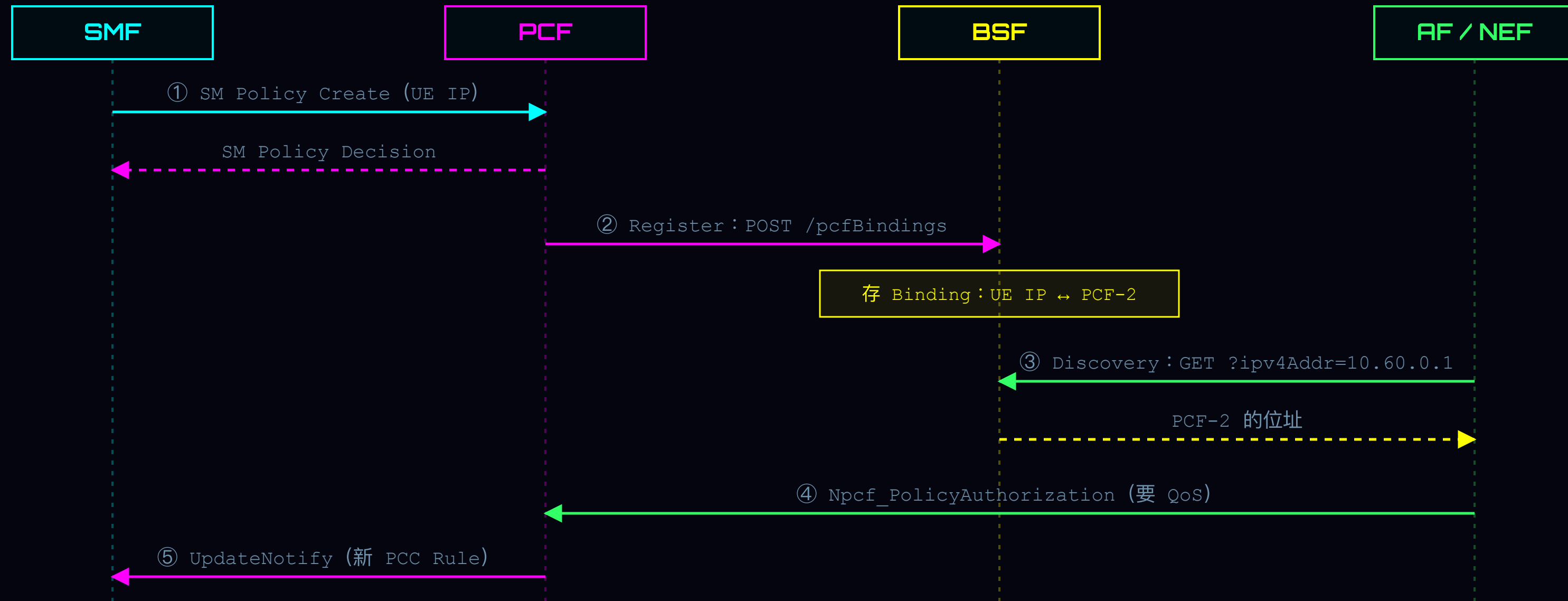
Update / Deregister

Discovery：用 UE IP 查

Subscribe：變更通知

BSF 不做策略決策，只是一個專門的查詢服務；也可以和 PCF 或 UDR 部署在一起。

/> BSF 在流程中的位置



➤ 一筆 PCF BINDING

```
POST /nbsf-management/v1/pcfBindings
{
  "supi": "imsi-208930000000001",
  "ipv4Addr": "10.60.0.1",
  "dnn": "internet",
  "snssai": { "sst": 1, "sd": "010203" },
  "pcfFqdn": "pcf.free5gc.org",
  "pcfIpEndpoints": [{ "ipv4Address": "127.0.0.7" }],
  "pcfId": "..."
}
→ 201 Created
Location: ../pcfBindings/{bindingId}
```

dnn、snssai 必填

UE 位址三選一

回傳 bindingId

PCF 記住這個 ID

/> FREE5GC BSF 的 API

路徑 (/NBSF-MANAGEMENT/V1)	方法	用途
/pcfBindings	POST · GET	PDU Session 的 Binding：登記 / 查詢
/pcfBindings/{bindingId}	GET · PATCH · DELETE	讀取、更新、刪除單筆
/pcf-ue-bindings	POST · GET	UE 層級的 Binding（AM / UE Policy）
/pcf-mbs-bindings	POST · GET	多播廣播（MBS）Session
/subscriptions	POST · PUT · DELETE	訂閱 Binding 變更

資料存在 MongoDB；另外有 Prometheus metrics（預設 :9091）可以觀察 Binding 數量。

➤ BSF 的檢查規則（依 TS 29.521）

1

缺 dnn 或 snssai

400 MANDATORY_IE_MISSING

2

同樣組合已經有 Binding

403 BINDING_ALREADY_EXISTS，避免兩個 PCF 搶同一條 Session

3

查詢時 ipv4Addr / ipv6Prefix / macAddr48

只能帶其中一個，否則 400

4

ipDomain

只能和 ipv4Addr 一起出現（私有 IP 可能重複）

➤ PCF 端：什麼時候寫 BSF？

```
// pcf/internal/sbi/processor/smpolicy.go
SM Policy Create:
    id, _ := Consumer().RegisterPCFBinding(smPolicy)
    smPolicy.BsfBindingId = id

SM Policy Update:
    Consumer().UpdatePCFBinding(id, smPolicy)

SM Policy Delete:
    Consumer().DeletePCFBinding(id)

// 失敗只記 Warn，不影響 Session
```

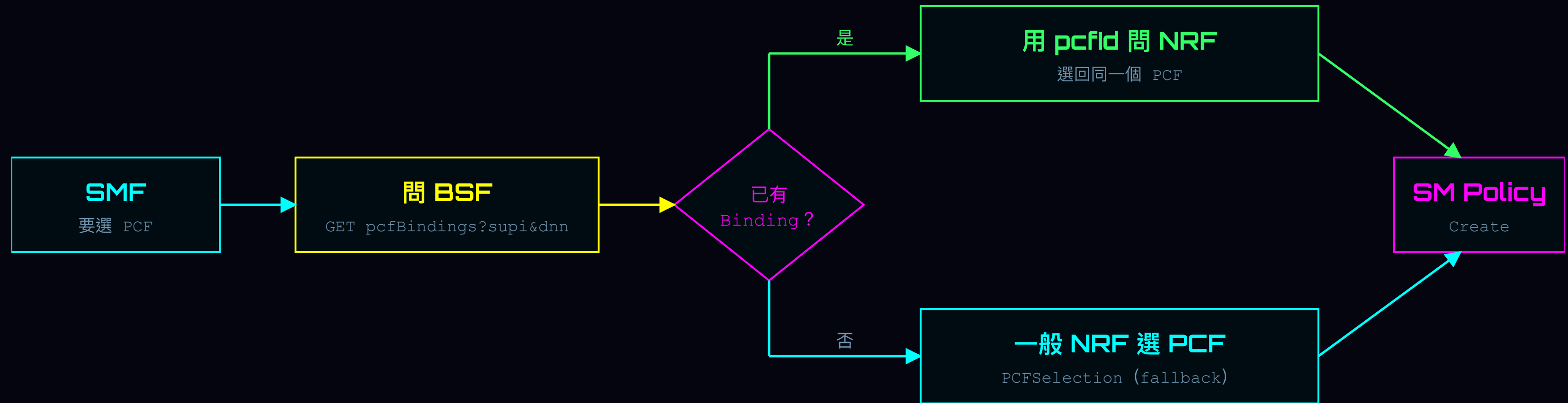
`bsf.enable` 控制開關

BSF 經 NRF 找到

找不到 → fallback

BSF 不是必要路徑

➤ SMF 端：選 PCF 時先問 BSF



free5GC SMF:BSFAwarePCFSelection() → PCFSelectionWithBSF(), 找不到就退回傳統作法

➤ 在 FREE5GC 開啟 BSF

```
# 1. 啟動時加參數
./run.sh -bsf

# 2. PCF 設定 (預設已是 true)
# config/pcfcfg.yaml
bsf:
  enable: true
```

```
# config/bsfcfg.yaml
sbi:
  registerIPv4: 127.0.0.15
  port: 8000
nrfUri: http://127.0.0.10:8000
mongodb:
  name: free5gc
metrics:
  enable: true
  port: 9091
```

run.sh 裡 SCP、BSF 都是 opt-in：不加參數時不會啟動，PCF 找不到 BSF 就照舊運作。

\$ PART 08



Charging Function：收集使用量、控制額度、產生計費紀錄

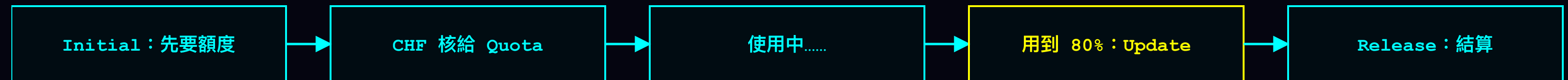
/> CHF 做什麼？



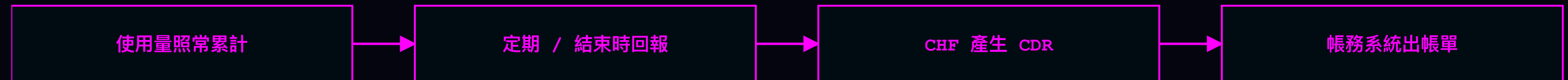
CHF 整合了 4G 的 OCS（線上）與 OFCS（離線），所以服務叫 Converged Charging。

/> 線上與離線計費

Online (預付 / 即時控制)：先拿額度才能用



Offline (後付)：先用，事後記帳



／> 計費的維度

TIME

時間

依使用時間，例如通話分鐘數

VOLUME

流量

依資料用量，例如 GB

EVENT

事件

依次數，例如一則簡訊

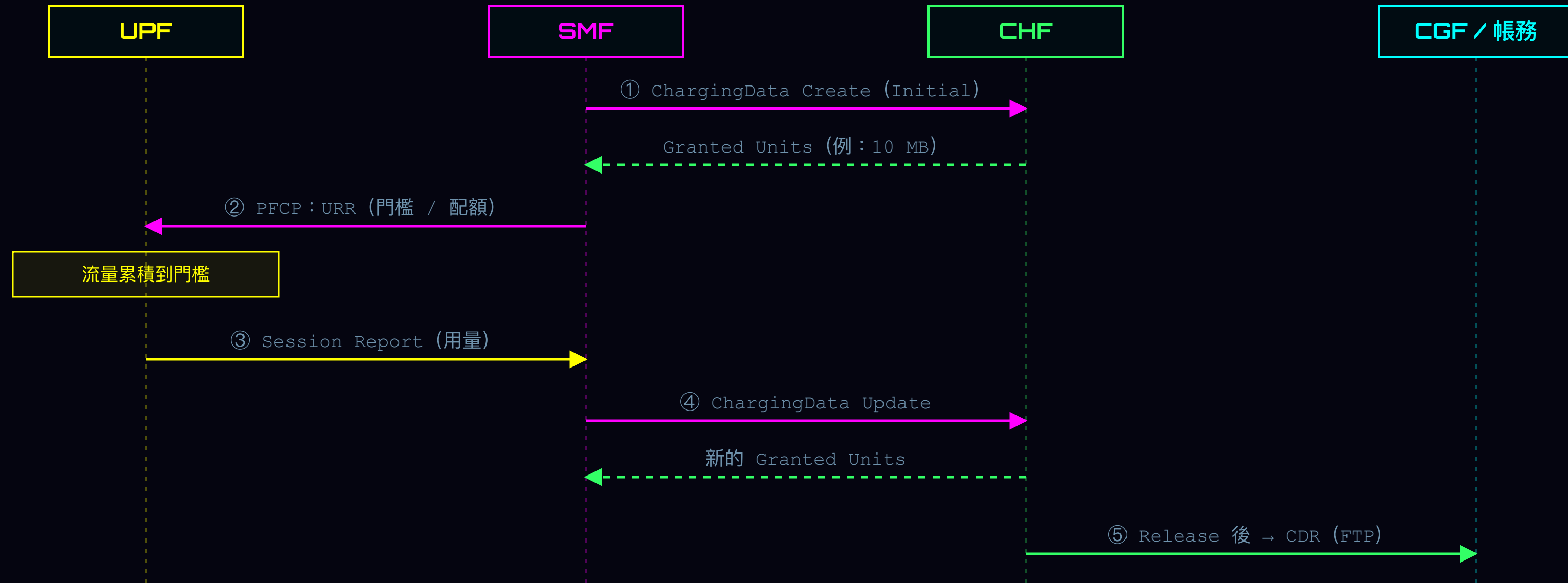
SERVICE

服務

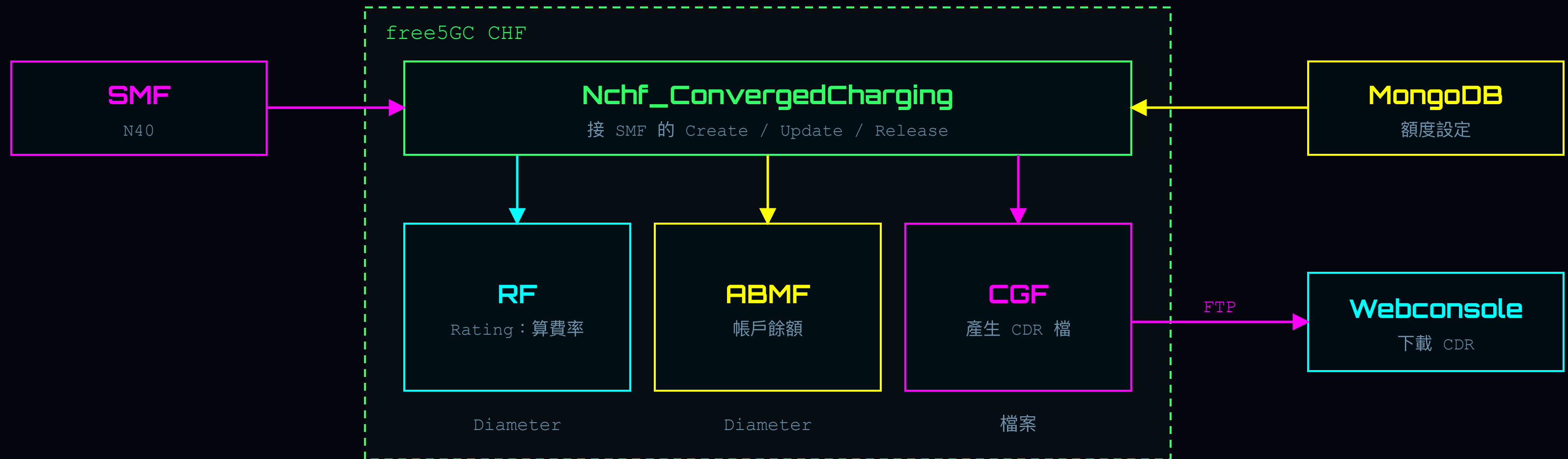
依服務類型，例如影音免計費

同一條 Session 裡不同服務可以有不同費率：用 Rating Group 區分，對應到 UPF 上不同的 URR。

➤ SMF、UPF、CHF 怎麼配合？



/> FREE5GC CHF 的內部



➤ FREE5GC CHF 的設定

```
# config/chfcfg.yaml (節錄)
serviceNameList:
  - nchf-convergedcharging
quotaValidityTime: 10000
volumeLimit: 50000
volumeLimitPDU: 10000
volumeThresholdRate: 0.8
cgf:
  enable: true
  hostIPv4: 127.0.0.1    # 帳務 FTP Server
  port: 2121
  cdrFilePath: /tmp
abmfDiameter: { port: 3868 }
rfDiameter:   { ... }
```

額度、門檻在這裡調

0.8 → 用到 80% 再要

CDR 先寫 /tmp

再由 FTP 給帳務系統

\$ PART 09

NSSF

Network Slice Selection Function：協助選擇合適的網路切片

／> 網路切片是什麼？

eMBB · SST 1

高頻寬：影音、AR / VR

URLLC · SST 2

低延遲高可靠：工廠、遠端控制

mMTC · SST 3

大量連線：感測器、IoT

同一套實體網路（RAN、傳輸、5GC）

➤ S-NSSAI 的結構

SST	SD
8 bits · 切片大類	24 bits · 同一類下的不同實例（選填）

1 = eMBB 、 2 = URLLC

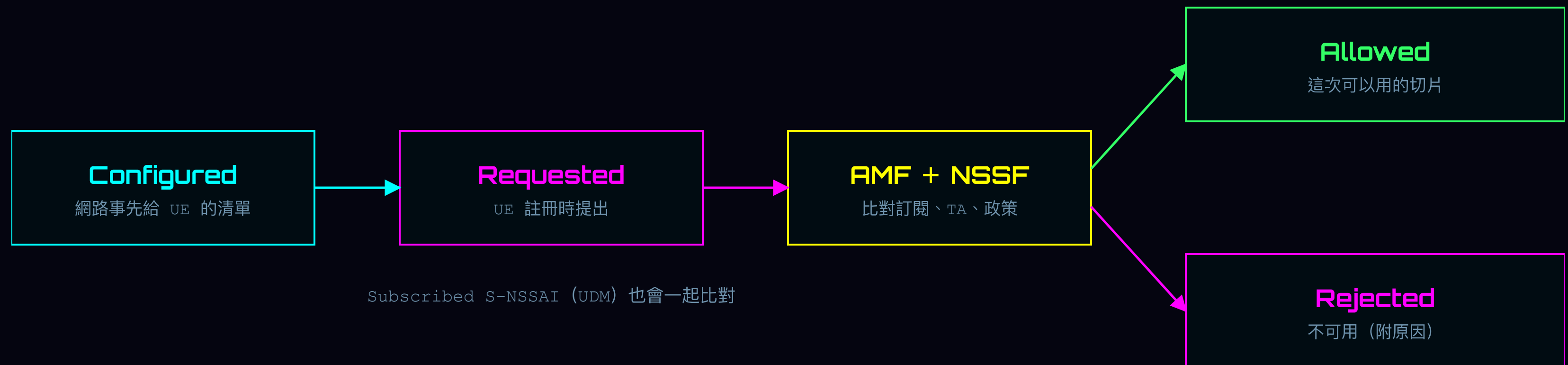
3 = MIoT 、 4 = V2X

營運商也可自訂

```
# free5GC 預設 UE
sst: 1, sd: "010203"
sst: 1, sd: "112233"
```

原文把 SD 稱為 SSD；3GPP 標準名稱是 SD（Slice Differentiator）。

➤ NSSAI 的四種狀態



/> NSSF 做什麼？

NSSelection

/nnssf-nssselection

決定 Allowed NSSAI

選 NSI、AMF Set

建 Session 時也可查

NSSAIAvailability

/nnssf-nssaiavailability

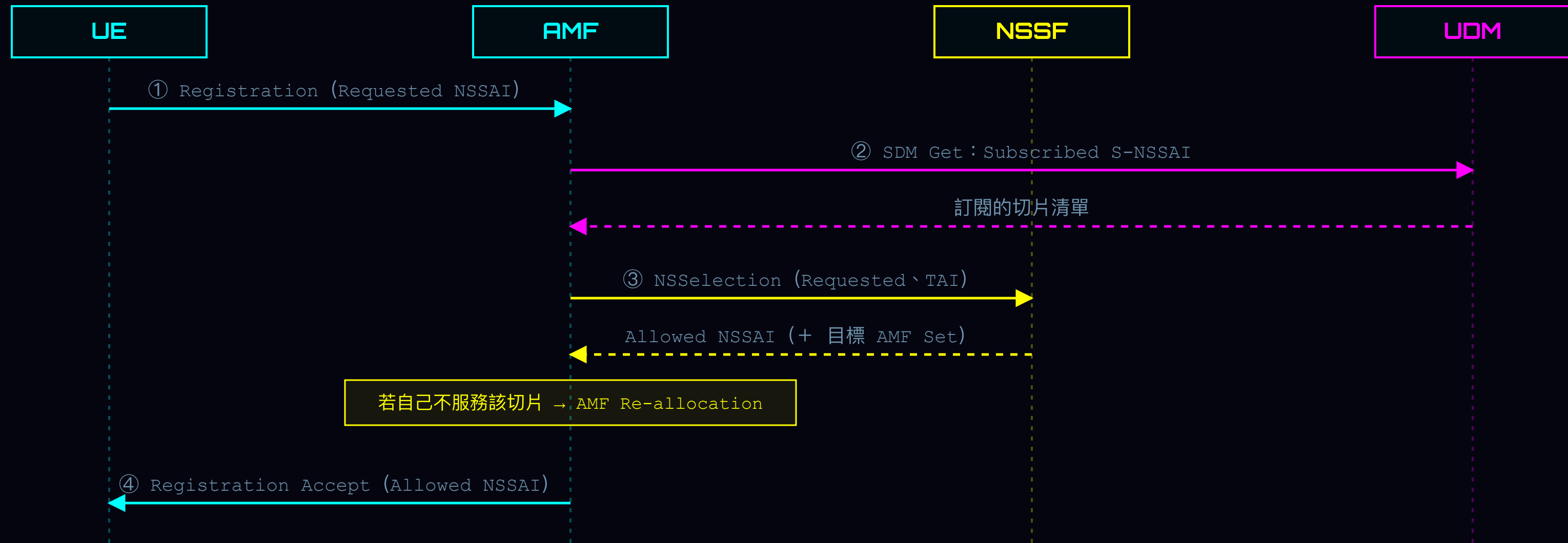
AMF 回報 TA 支援的切片

NSSF 掌握全網切片分布

可訂閱變更通知

AMF 與 NSSF 之間是 N22 介面；同一套 5GC 就能服務不同客戶與業務。

／> 註冊時的切片選擇



➤ FREE5GC 的 NSSF 設定

```
# config/nssfcfg.yaml (節錄)
supportedNssaiInPlmnList:
  - plmnId: { mcc: 208, mnc: 93 }
    supportedSnssaiList:
      - { sst: 1, sd: 010203 }
      - { sst: 1, sd: 112233 }
      - { sst: 2, sd: 000001 }
nsiList:
  - snssai: { sst: 1 }
    nsiInformationList:
      - nrfId: http://127.0.0.10:8000/nnrf-nfm/v1/nf-instances
        nsiId: 10
```

PLMN 支援哪些切片

每個切片用哪個 NRF

還有 TA、AMF Set 設定

\$ PART 10



Network Exposure Function：把 5G 核心能力包裝成 API 對外開放

/> NEF 做什麼？

01

API 暴露

核心功能包成標準 API

02

資料暴露

安全地提供網路資訊

03

事件暴露

位置、連線狀態變化

04

參數提供

外部參數傳進核心網

05

安全管理

認證、授權、加密

06

速率限制

控制 API 呼叫頻率

07

資料翻譯

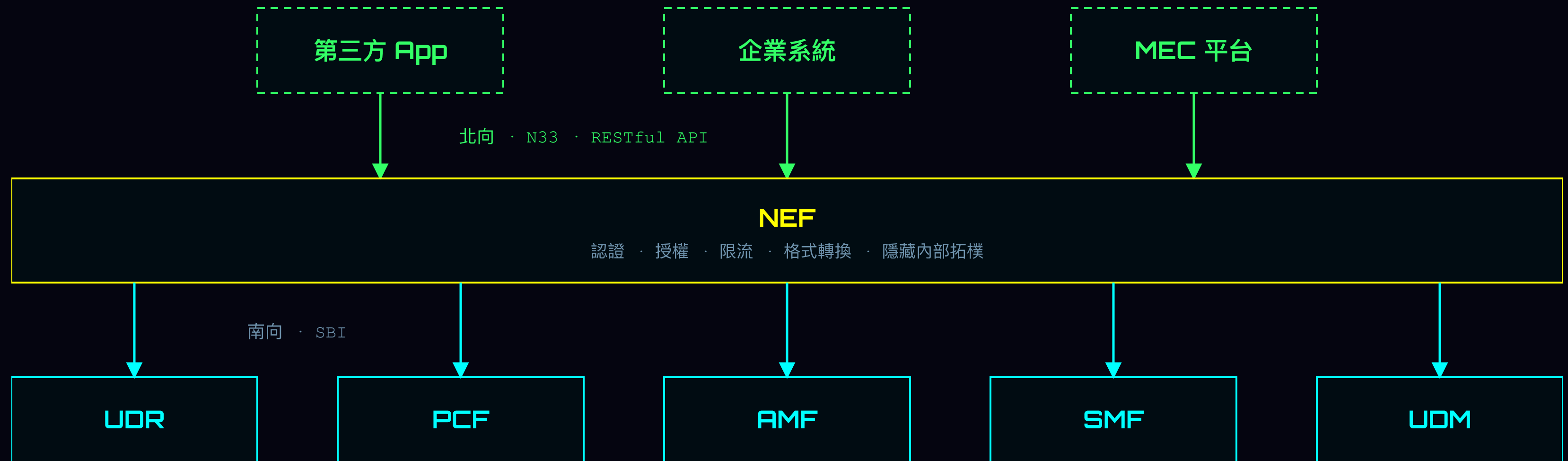
外部 API ↔ 內部 SBI

08

計費支援

API 使用量計費

➤ NEF：對外的窗口



/> NEF 的使用情境

01

第三方應用

開發者呼叫網路能力 API

02

邊緣運算

MEC 取得網路資訊、影響路由

03

企業應用

專網客製化服務

04

垂直行業

智慧製造、自動駕駛

對外 API 的統一框架是 CAPIF (TS 23.222)：API 的發布、發現與授權都有標準。

FREE5GC NEF 的 API

路徑	對象	用途
<code>/3gpp-traffic-influence/v1/{afId}/subscriptions</code>	AF (北向)	Traffic Influence (W6)
<code>/3gpp-pfd-management/v1/{scsAsId}/transactions</code>	AF (北向)	提供應用偵測規則 PFD
<code>/nnef-pfdmanagement/v1/...</code>	SMF (南向)	SMF 取得 PFD
<code>/nnef-callback/v1/notification/smf</code>	SMF (南向)	接收 SMF 的事件通知

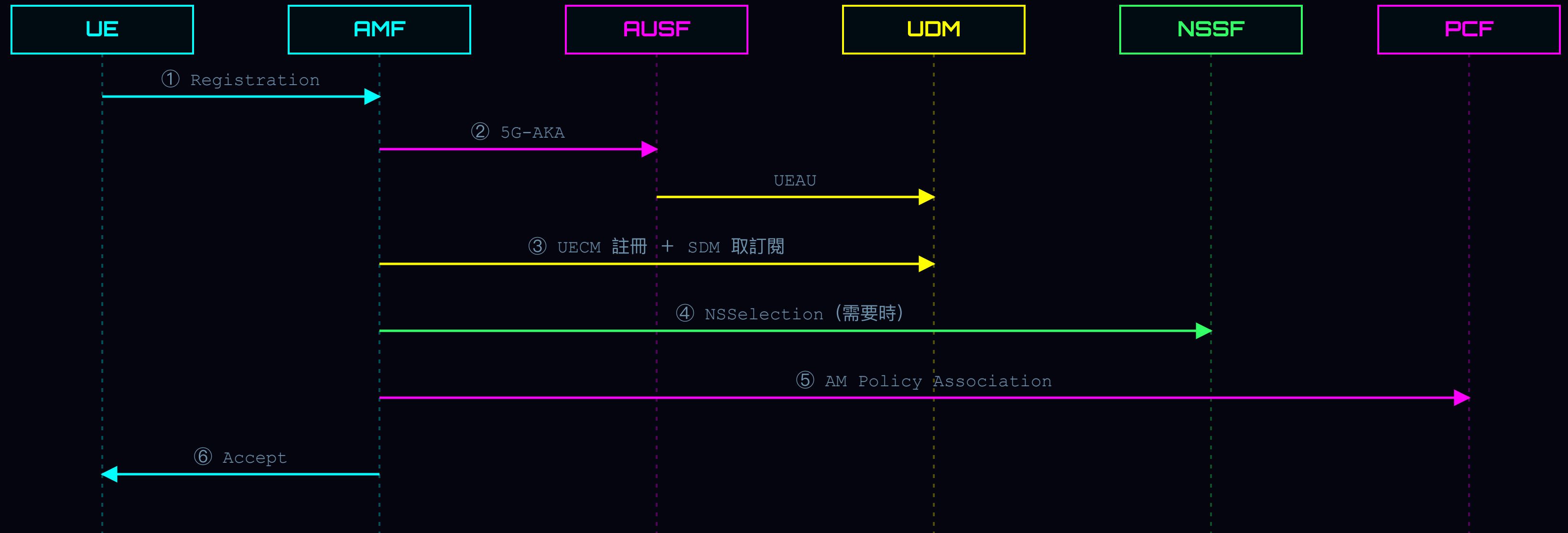
北向 API 以 3gpp- 開頭（給外部），南向以 nnef- 開頭（給核心網內的 NF）。

\$ PART 11

串起來

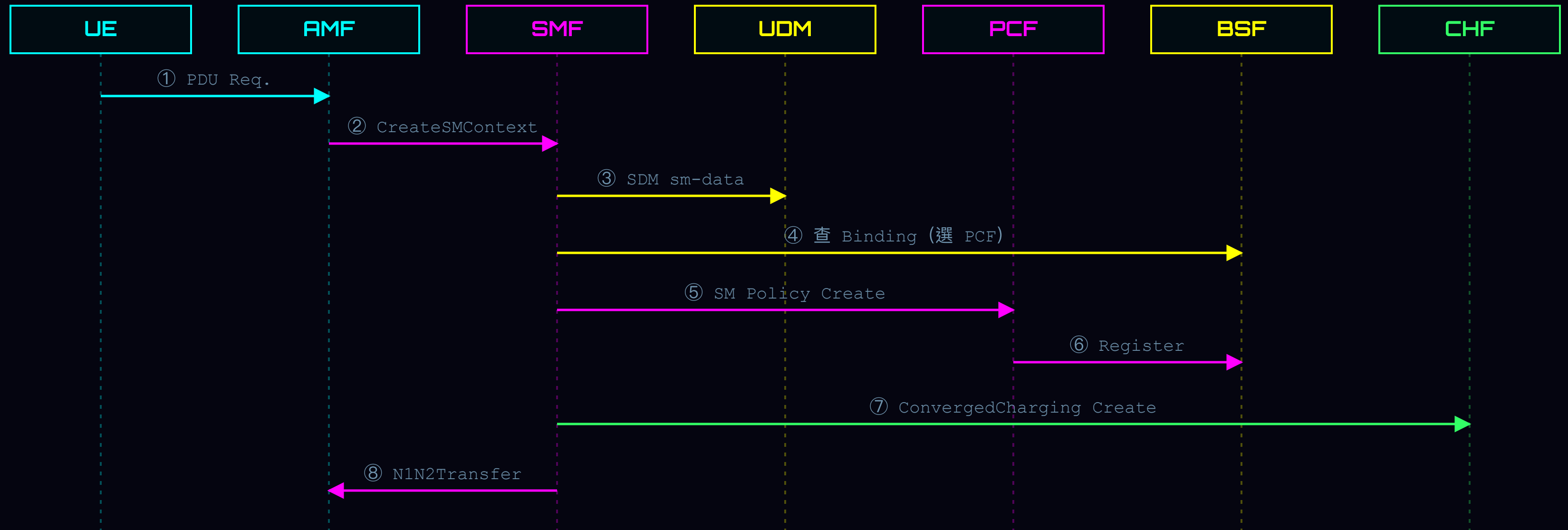
一次註冊、一次建 Session，會碰到哪些 NF？

一次註冊碰到的 NF



背後 UDM、PCF 都再去 UDR 讀資料。

一次建 SESSION 碰到的 NF



之後 UPF、gNB 的部分見 W6；開了 BSF 才會有 ④ ⑥。

NF 速查表

NF	一句話	FREE5GC SBI
NRF	服務登錄與發現、簽發 Token	127.0.0.10
SCP	轉送代理 (opt-in)	127.0.0.6
AUSF	認證	127.0.0.9
UDM	用戶資料的邏輯	127.0.0.3
UDR	統一資料庫	127.0.0.4
PCF	策略	127.0.0.7
BSF	Session ↔ PCF 對照 (opt-in)	127.0.0.15
CHF	計費與配額	127.0.0.113
NSSF	切片選擇	127.0.0.31
NEF	能力對外開放	127.0.0.5

➤ PART A 小結

NRF 讓 NF 互相找得到；SCP 讓訊息可以集中轉送

AUSF + UDM 完成 5G-AKA，Home 網路握有最後決定權

UDM 會思考、UDR 會存東西；Webconsole 直接寫 MongoDB

PCF 出策略、BSF 記住 Session 由哪個 PCF 管、CHF 管錢

NSSF 選切片、NEF 把能力開放給外部

休息一下，接著是 Part B：非 3GPP 接入

\$ PART 8 · NON-3GPP ACCESS

➤ 非 3GPP 接入

透過 Wi-Fi 接入 5G 核心網路：N3IWF、TNGF 與 ATSSS

/> PART B 大綱

B1

為什麼

Wi-Fi 也能進 5GC

B2

N3IWF

不可信任：IPsec /
IKEv2

B3

TNGF

可信任：802.1X +
EAP-5G

B4

TWIF

不會講 NAS 的 Wi-Fi
裝置

B5

ATSSS

3GPP + Wi-Fi 同時用

／> 為什麼要讓 WI-FI 進 5GC？

01

Wi-Fi 到處都有

家裡、辦公室、咖啡店，已經有現成的接入網

02

補室內覆蓋

高頻 5G 穿牆差，室內靠 Wi-Fi 補

03

統一核心網

同一套訂閱、認證、策略、計費，不管從哪裡接入

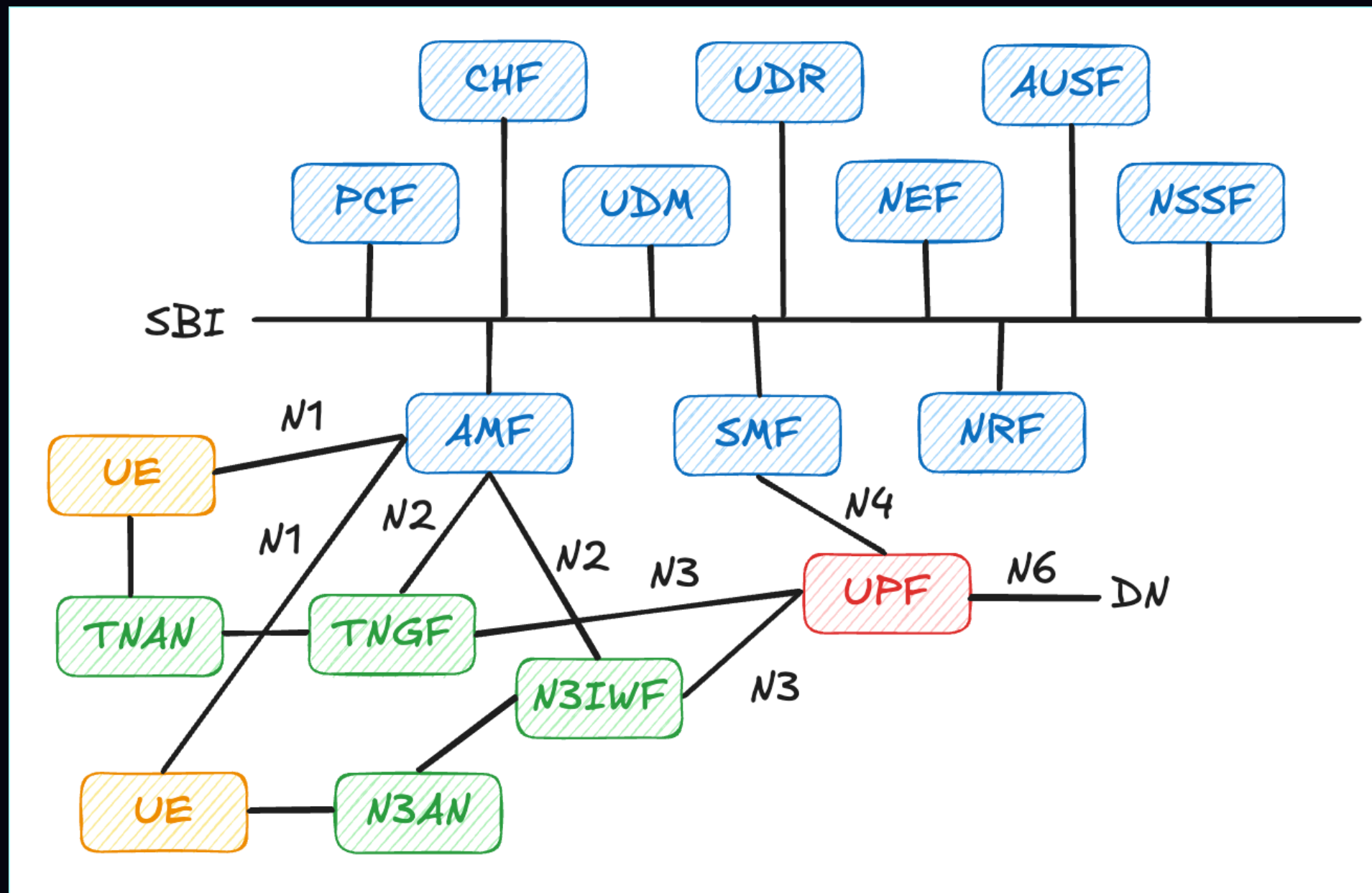
04

多路徑

5G 和 Wi-Fi 同時用，更快、更可靠（ATSSS）

4G 也有類似設計（ePDG、TWAG），但 5G 讓非 3GPP 接入直接接到 AMF / UPF，和 RAN 一樣。

➤ 非 3GPP 接入的架構



TNAN + TNGF : 可信任

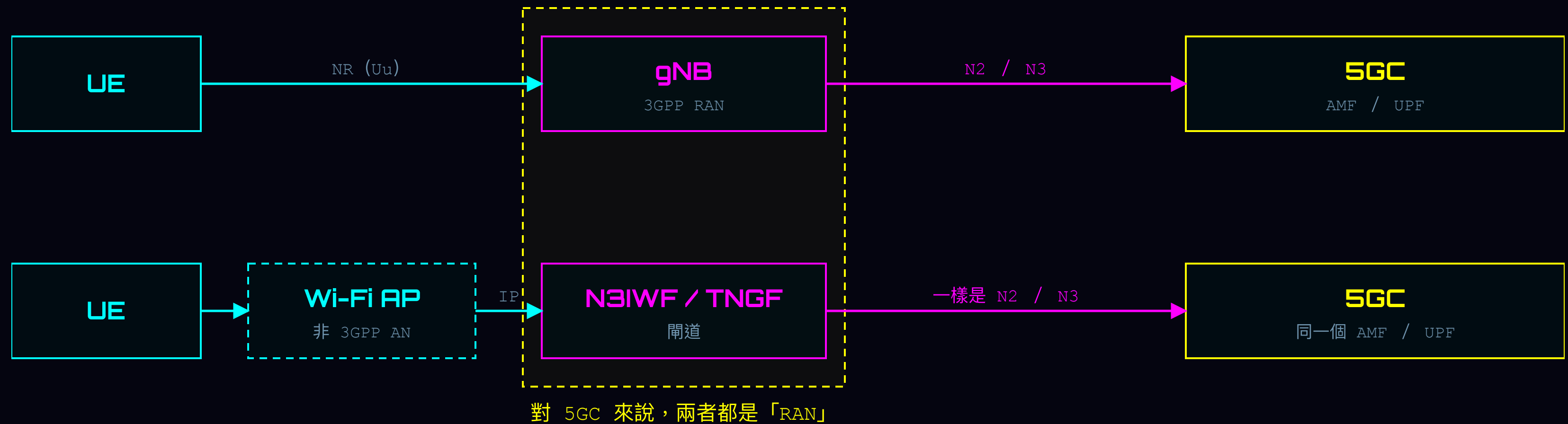
N3AN + N3IWF : 不可信任

都接 AMF (N2)

都接 UPF (N3)

N1 仍到 AMF

／> 對 5GC 來說，這是另一種 RAN



／> 可信任與不可信任

可信任 · TNGF

Trusted Non-3GPP

營運商自建的 Wi-Fi 熱點
與營運商共同規劃的專網
Wi-Fi 本身就可以信任
視為 RAN 的延伸

不可信任 · N3IWF

Untrusted Non-3GPP

公共 Wi-Fi、咖啡店熱點
家用路由器
中間網路完全不可信
必須自己加密到底

「可不可信任」是營運商的判斷，不是技術本身決定的：同一顆 AP 也可以被當成不可信任。

➤ 和 4G 對照

比較	4G EPC	5GC
不可信任閘道	ePDG	N3IWF
可信任閘道	TWAG	TNGF
接到哪裡	P-GW (S2b / S2a)	AMF (N2) + UPF (N3)
NAS / 移動性	Wi-Fi 側沒有 NAS	和 3GPP 一樣走 NAS 註冊
認證	經 AAA (SWm / STa)	同一套 AUSF / UDM

\$ PART 02

N3IWF

Non-3GPP InterWorking Function：專門為 5G UE 準備的 VPN Gateway

➤ N3IWF 的整體流程

1

連上任何 IP 網路

Wi-Fi 或有線，取得 IP，跟一般上網一樣

2

IKEv2 / IPsec 交握

UE 與 N3IWF 建立加密通道

3

隧道裡跑 NAS

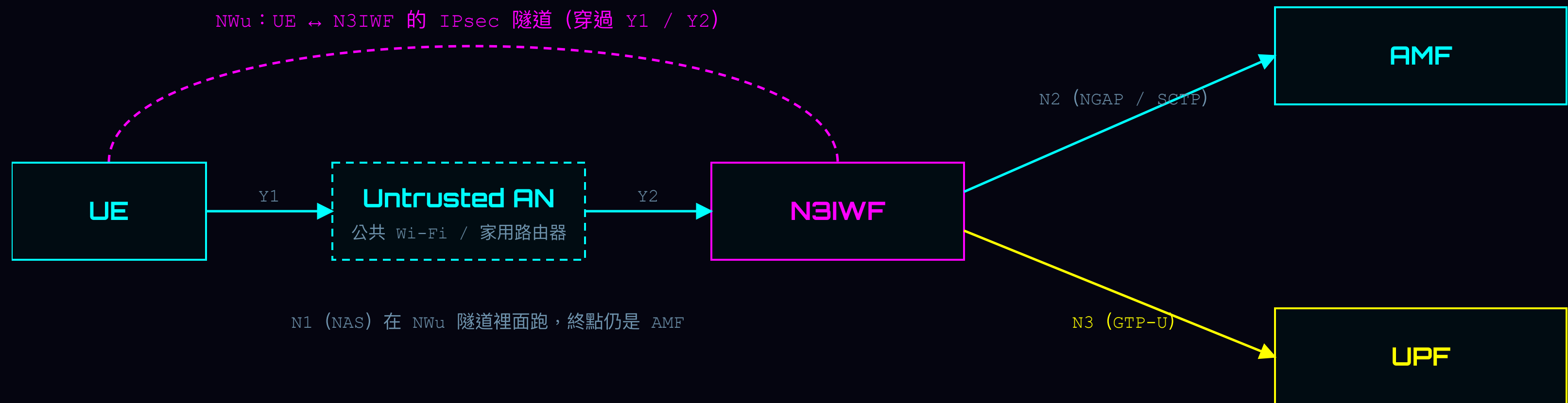
UE 與 AMF 交換訊息，等於遠端連入 5GC

4

註冊、建 Session、傳資料

全部在隧道內封裝與轉送

➤ N3IWF 的介面



/> IKEV2 / IPSEC 速覽

交換	做什麼	在 N3IWF 裡
IKE_SA_INIT	DH 交換，建立加密的 IKE SA	還不知道對方是誰
IKE_AUTH	認證雙方，建立第一個 SA	用 EAP-5G 夾帶 NAS 註冊
CREATE_CHILD_SA	再開新的 IPsec SA	每個 PDU Session 的使用者面
INFORMATIONAL	刪除 SA、存活檢查 (DPD)	livenessCheck

IKE 走 UDP 500，遇到 NAT 改走 UDP 4500 (NAT-T)，資料用 ESP 加密。

➤ EAP-5G：還沒有隧道，NAS 怎麼送？

問題

雞生蛋

IPsec SA 要先認證才能建

認證要靠 NAS 和 AMF 談

但 NAS 要走 IPsec.....

解法

TS 24.502

在 IKE_AUTH 裡夾帶 EAP

EAP-5G 是 3GPP 自訂的 EAP

5G-Start / 5G-NAS / 5G-Stop

NAS 就放在 5G-NAS 裡

EAP-5G 只是「搬運 NAS 的信封」；真正的認證方法仍是 5G-AKA 或 EAP-AKA'。

➤ 隧道裡裝了什麼？

控制面 (Signalling SA)

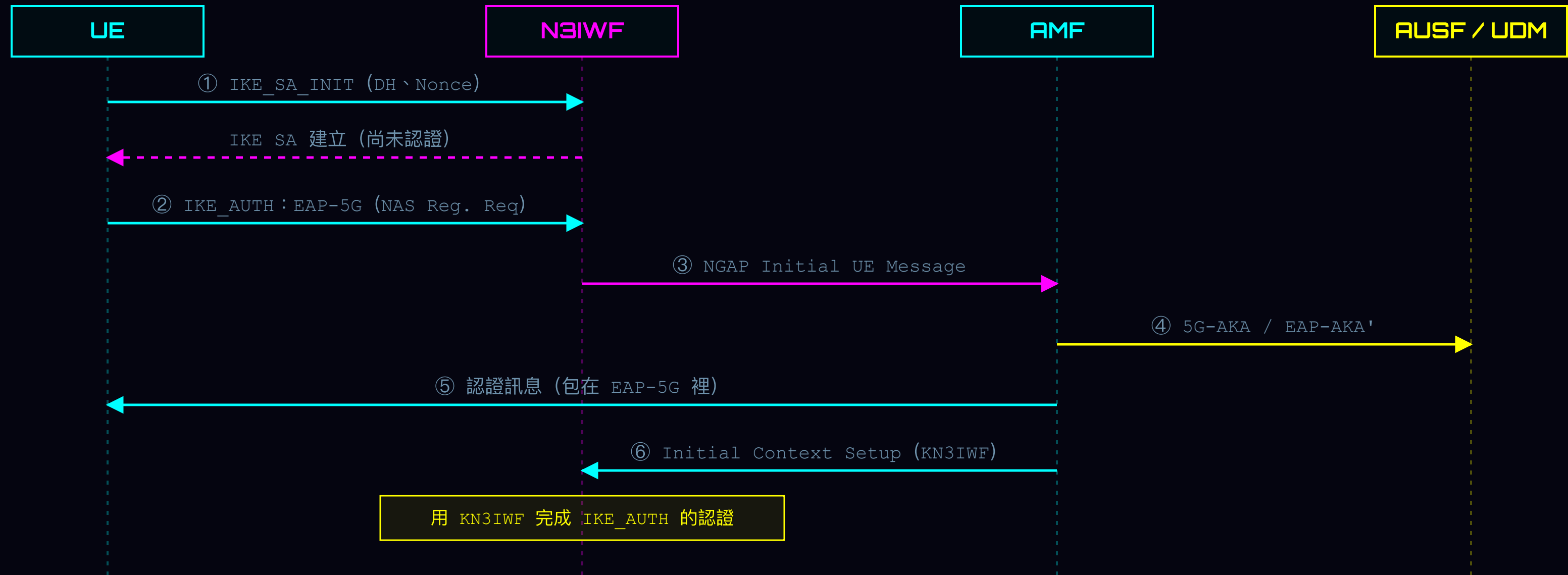
NAS (5GMM / 5GSM)	給 AMF
TCP :20000	nasTcpPort
內層 IP	10.0.0.x
IPsec ESP	加密
外層 IP	Wi-Fi 拿到的 IP
Wi-Fi L2	

使用者面 (Child SA)

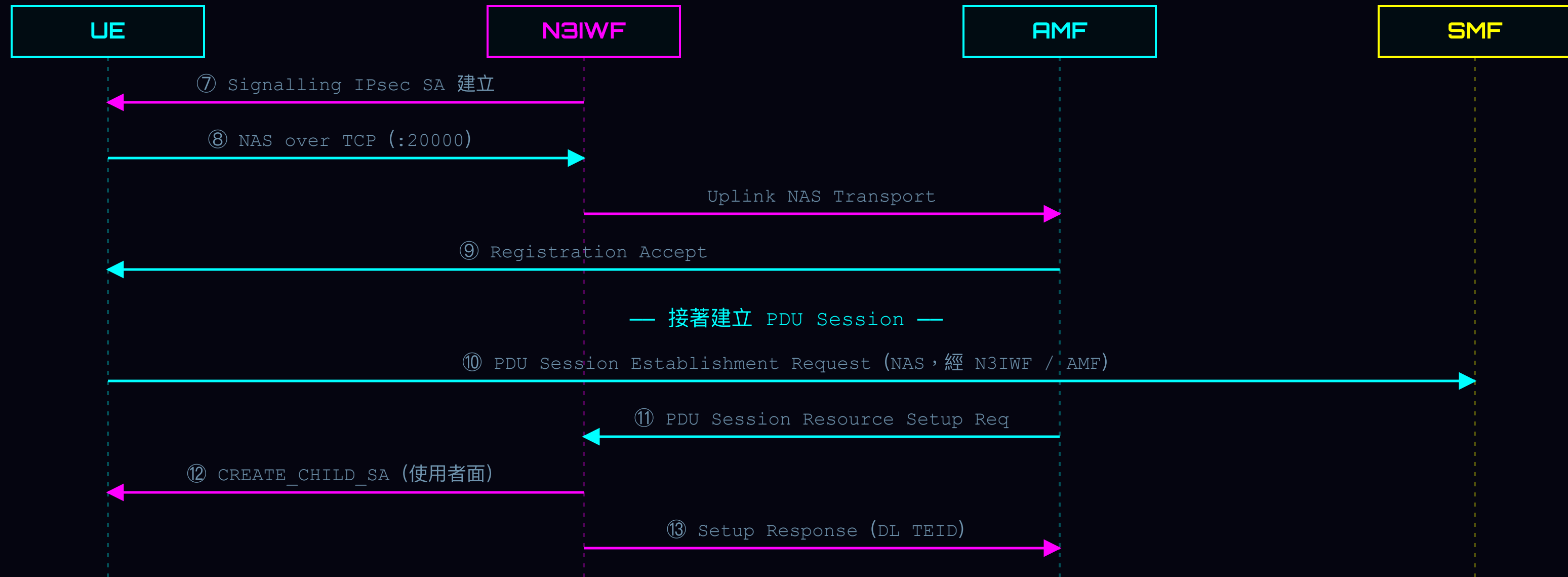
使用者 IP 封包	10.60.0.x
GRE	Key 帶 QFI
內層 IP	
IPsec ESP	加密
外層 IP	
Wi-Fi L2	

N3IWF 解開 ESP 與 GRE 之後，再用 GTP-U 送往 UPF：對 UPF 來說和 gNB 送來的一模一樣。

／> 經 N3IWF 註冊（上）



／> 經 N3IWF 註冊（下）與建 SESSION



➤ 雙層防護

外層：IPsec / IKEv2

憑證與金鑰建立加密隧道：中間網路再不可信，也無法竊聽或竄改

內層：5G-AKA / EAP-AKA'

向 AUSF / UDM 證明身分：決定「你是誰、能不能用這張網」

NAS 訊息 + 使用者資料

實驗可以用自簽憑證；接近實務時要用正式 PKI，嚴格管理 N3IWF 的憑證與金鑰，別讓它變成入口。

➤ FREE5GC 的 N3IWF

```
# config/n3iwfcfg.yaml (節錄)
amfSCTPAddresses:
  - ip: [127.0.0.18]
    port: 38412          # N2
nasTcpPort: 20000        # 隧道內的 NAS
ikeBindAddress: 172.16.2.100 # NWu (IKE)
ipSecTunnelAddress: 10.0.0.1
ueIpAddressRange: 10.0.0.0/24 # 內層 IP
xfrmInterfaceName: xfrmi
n3iwfGtpBindAddress: 127.0.0.33 # N3
livenessCheck:
  enable: true          # DPD
```

```
./run.sh -n3iwf
```

需要 sudo (XFRM)

模組：ike、nwucp、nwwup、gre、gtp、
ngap

➤ 把 N3IWF 想成 VPN GATEWAY

比較	企業 VPN	N3IWF
隧道技術	IPsec / IKEv2	IPsec / IKEv2 (相同)
認證誰	員工帳號	USIM (5G-AKA)
隧道裡跑	企業內網流量	NAS + 使用者面
後面接到	公司內網	AMF (N2) 與 UPF (N3)

\$ PART B3

TNGF

Trusted Non-3GPP Gateway Function：營運商可以信任的 Wi-Fi

➤ TNGF 負責什麼？

01

通道

經非 3GPP 網路建立並維護控制面與使用者面通道

02

協調 5GC

和 AMF / SMF 協調註冊與 PDU Session

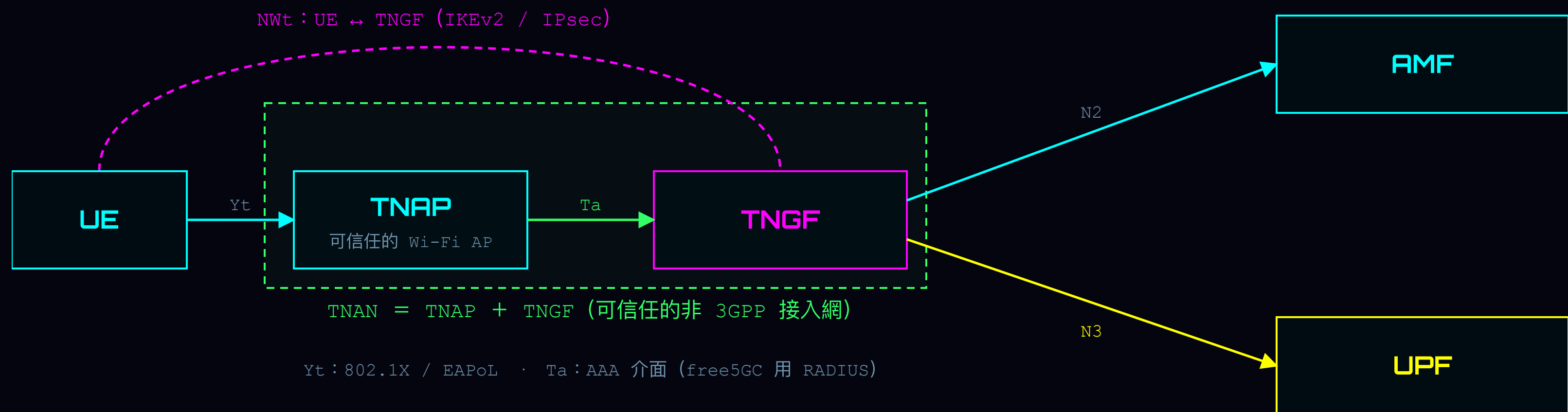
03

接入認證

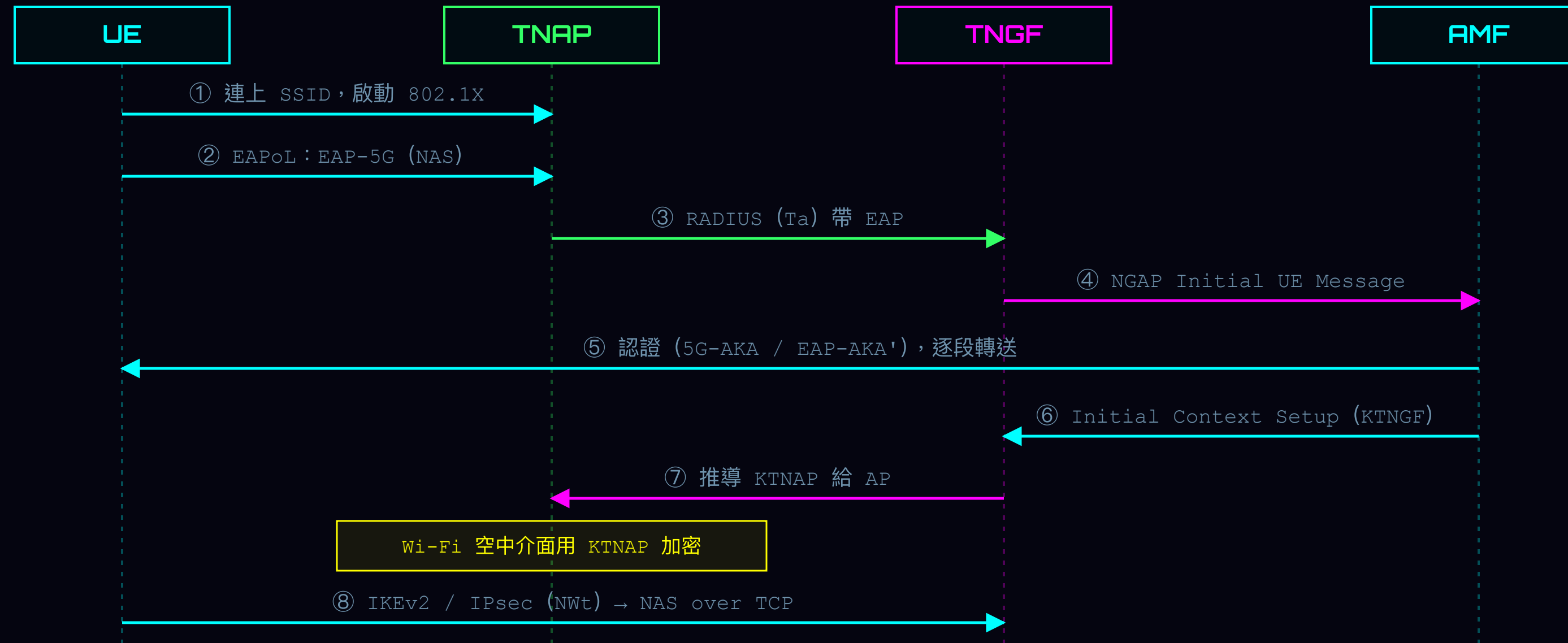
和 Wi-Fi 端的 AAA 配合，完成 UE 的接入驗證

Wi-Fi 可以被營運商視為「自己的延伸」時，就走 TNGF 這條路。

➤ TNGF 的架構



／> 經 TNGF 註冊



／> 可信任，不代表不設防

接入層

企業級 WI-FI

802.1X、WPA2 / WPA3-Enterprise，串營運商
AAA

邊界

網段隔離

TNGF 所在網段與其他 IT 網路以防火牆區隔

核心

TLS / IPSEC

TNGF 與 5GC 的 N2 / N3 / SBI 仍要憑證保護

NWt 上的 IPsec 可用 NULL 加密：空中介面已由 Wi-Fi (KTNAP) 加密，不必再加密一次。

➤ FREE5GC 的 TNGF

```
# config/tngfcfg.yaml (節錄)
NASTCPort: 20000
IKEBindAddress: 192.168.1.102
RadiusBindAddress: 192.168.1.102    # Ta
RadiusSecret: free5gctngf
IPSecTunnelAddress: 10.0.0.1
UEIPAddressRange: 10.0.0.0/24
XFRMInterfaceName: xfrmi
```

```
./run.sh -tngf
```

內建 RADIUS Server

AP 要設成用它認證

模組：nwtcp、nwtup、gre、gtp、ngap

\$ PART B4

TWIF

Trusted WLAN Interworking Function：讓不會講 NAS 的 Wi-Fi 裝置也能進 5GC
(free5GC 尚未實作，但私有 5G 網路很重要)

➤ N5CW：不會講 5G 的裝置

N5CW 裝置

Non-5G-Capable over WLAN

筆電、印表機、掃描槍

工廠裡只有 Wi-Fi 的感測器

沒有 5G 協定堆疊、沒有 NAS

只會 802.1X + EAP-AKA'

N3IWF / TNGF 不夠用

它們都假設 UE 會講 NAS

EAP-5G 裡裝的是 NAS

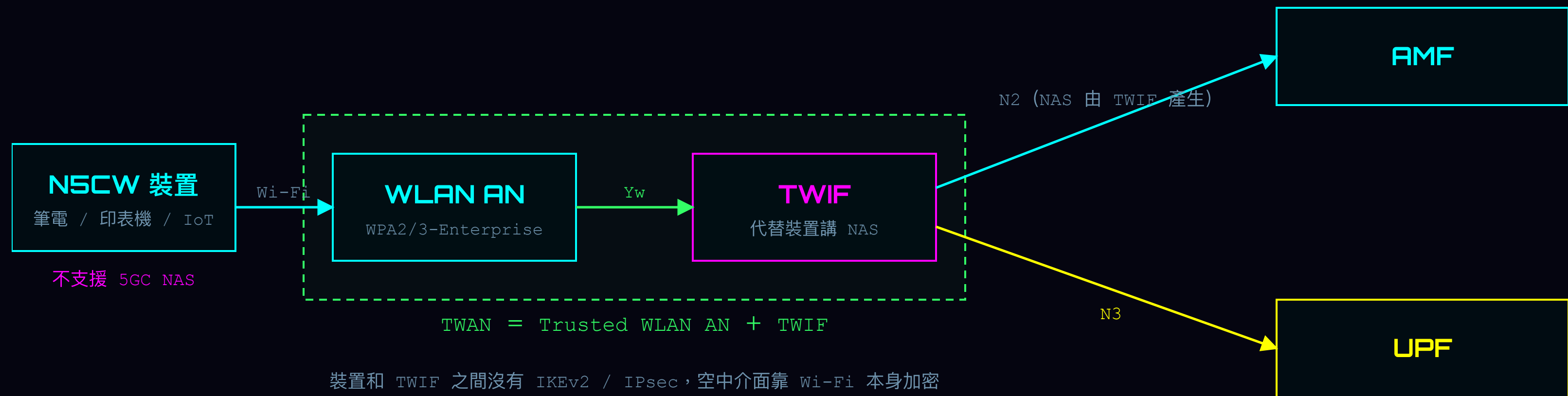
IKEv2 需要 UE 端軟體

這些裝置做不到

→ Rel-16 新增 TWIF

TS 23.501 §4.2.8.5、TS 23.502 §4.12b：由網路端的 TWIF 代替裝置執行 5GC 的程序。

➤ TWIF 的架構



/> NAS 由誰講？

N3IWF

不可信任

UE 自己講 NAS

走 IPsec 隧道

閘道只轉送

TNGF

可信任

UE 自己講 NAS

EAP-5G + IPsec

閘道只轉送

TWIF

可信任 · N5CW

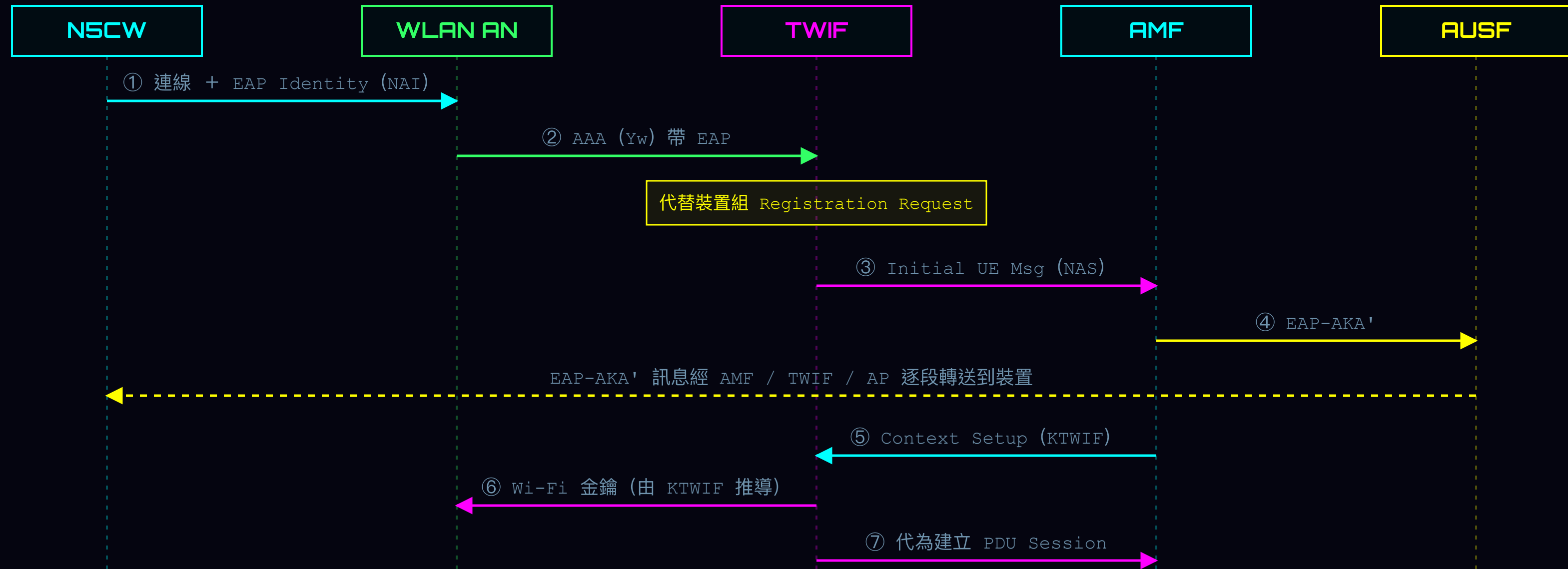
TWIF 代替裝置講 NAS

沒有隧道

閘道就是「UE 代理人」

對 AMF 來說，TWIF 送上來的註冊和一般 UE 沒兩樣；裝置本身完全不知道 5GC 的存在。

／> 經 TWIF 註冊與建 SESSION



⑧ 裝置用 DHCP 拿到 5GC 分配的 IP；資料走 Wi-Fi → TWIF → N3 → UPF。

／> 裝置沒說的，TWIF 來決定

一般 UE 會自己帶的	經 TWIF 時
身分 (SUCI)	由裝置的 NAI 轉成 SUCI
Requested NSSAI、DNN	TWIF 設定的預設值 (或依訂閱)
PDU Session 數量	通常每台裝置一條
QoS Rule	裝置看不到，由 TWIF / UPF 處理
Wi-Fi 金鑰	KTWIF 推導後交給 AP

／> 為什麼私有 5G 需要 TWIF？

01

Wi-Fi 裝置才是大宗

工廠、醫院、校園裡大量設備只有 Wi-Fi，不可能全部換成 5G 模組

02

一套身分與策略

5G 手機和 Wi-Fi 設備都由 UDM 認證、PCF 管策略

03

同一個出口

流量都從 UPF 出去：同一套 ULCL、MEC、計費與監控

04

裝置不用改

只要支援企業級 Wi-Fi (802.1X / EAP-AKA') 就能接入

free5GC 目前有 N3IWF、TNGF，還沒有 TWIF；這是一個值得投入的開源題目。

/> N3IWF、TNGF、TWIF 比較

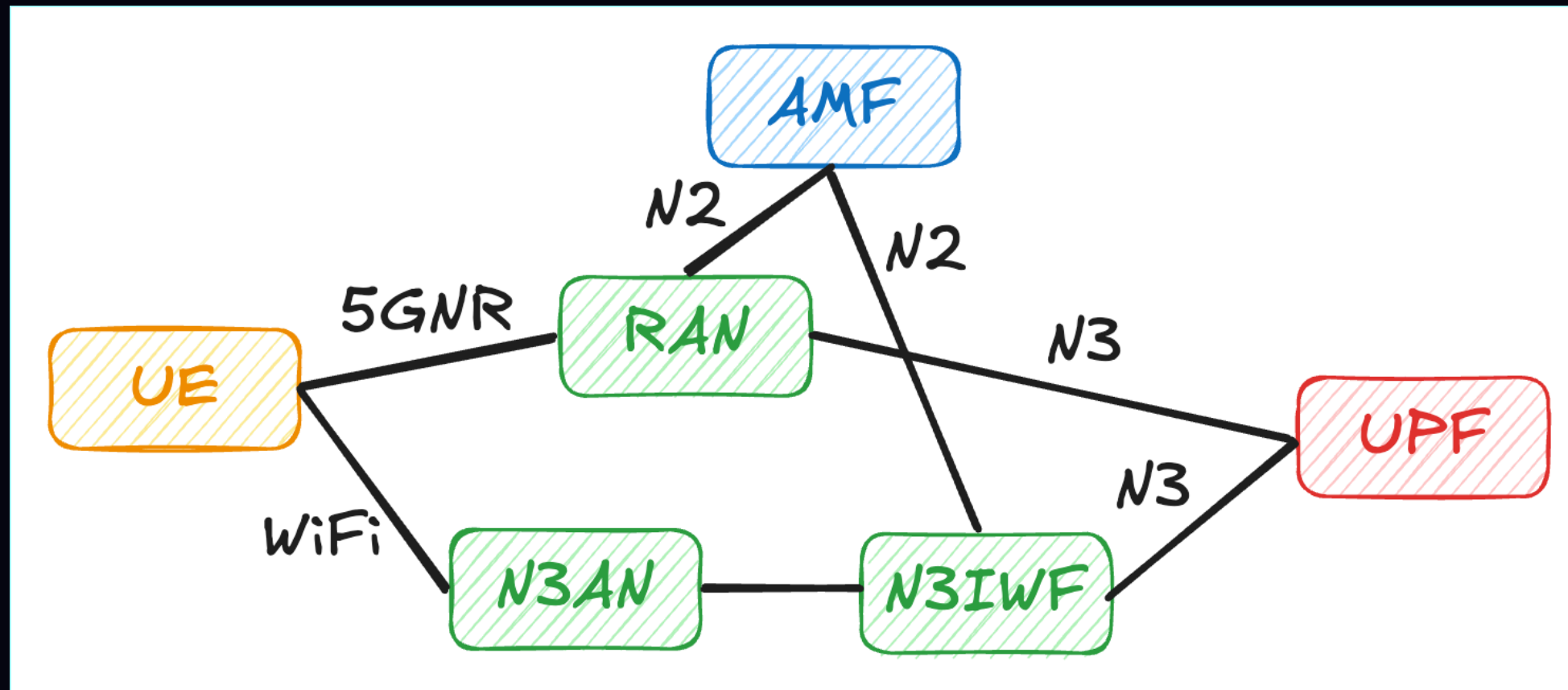
比較	N3IWF	TNGF	TWIF
信任前提	不信任 Wi-Fi	信任 Wi-Fi	信任 Wi-Fi
裝置講 NAS ?	要	要	不用 (TWIF 代講)
典型場景	公共 Wi-Fi、家用	營運商熱點、專網	私網的 Wi-Fi 設備
接入認證	IPsec 裡做	EAP-5G	EAP-AKA'
UE ↔ 開道	NWu : IPsec	NWt : IPsec (可 NULL)	無隧道
和 AP 的關係	AP 不知道 5GC	經 Ta 合作	經 Yw 合作
free5GC	有	有	尚未實作

\$ PART B5

ATSSS

Access Traffic Steering, Switching and Splitting：多接取路徑下的智慧流量控制

／> 同時用 5G 和 WI-FI

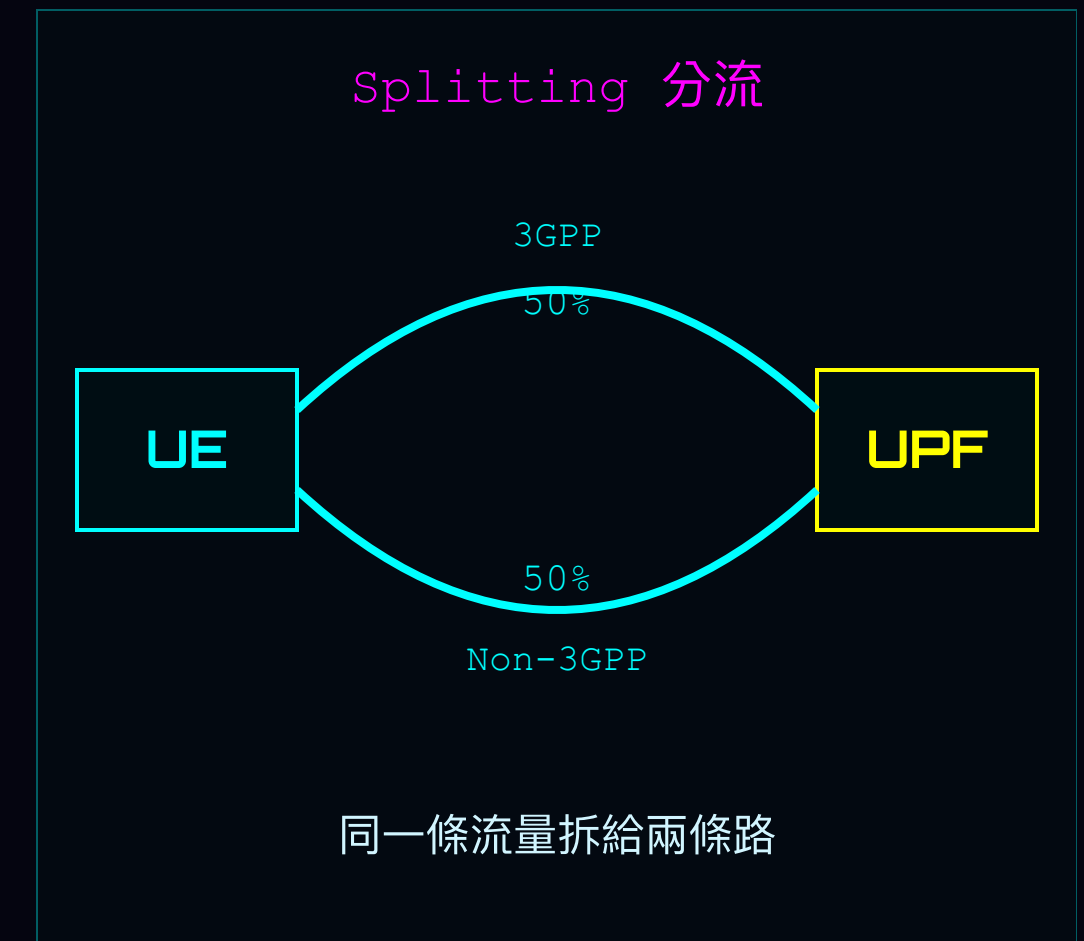
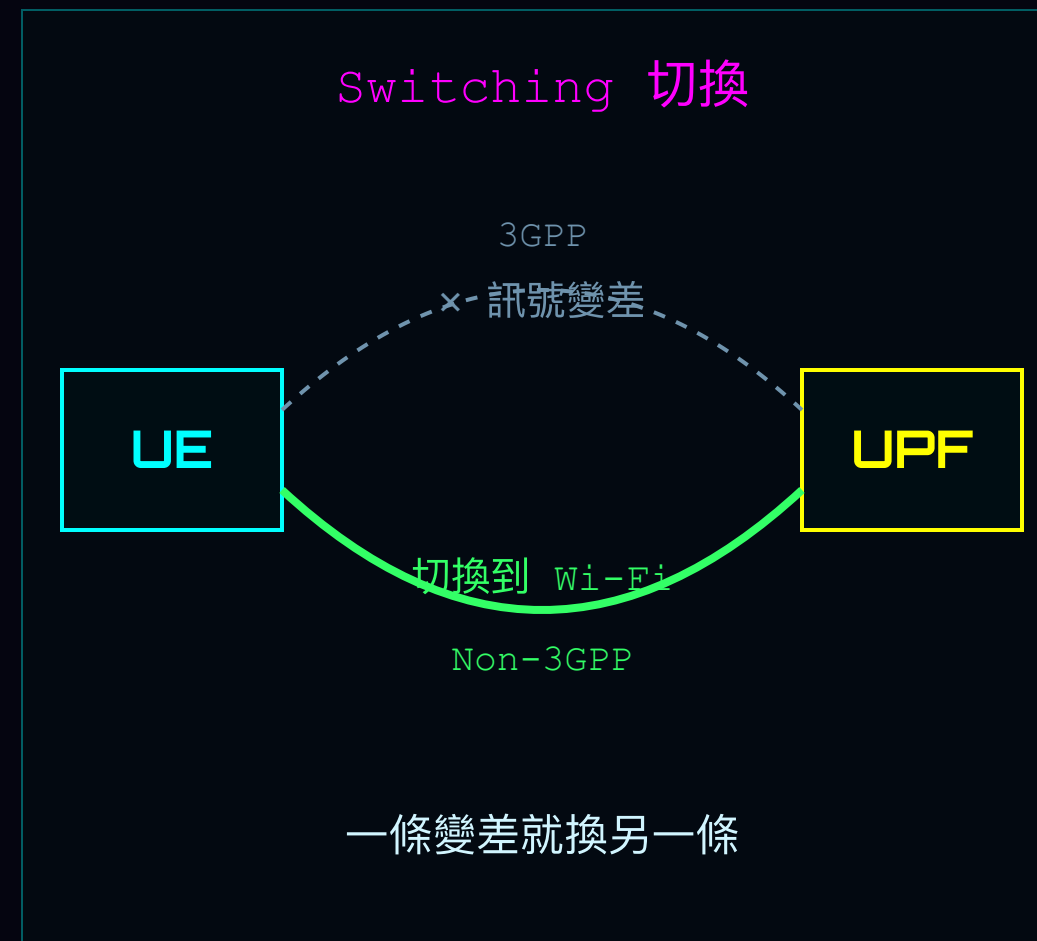
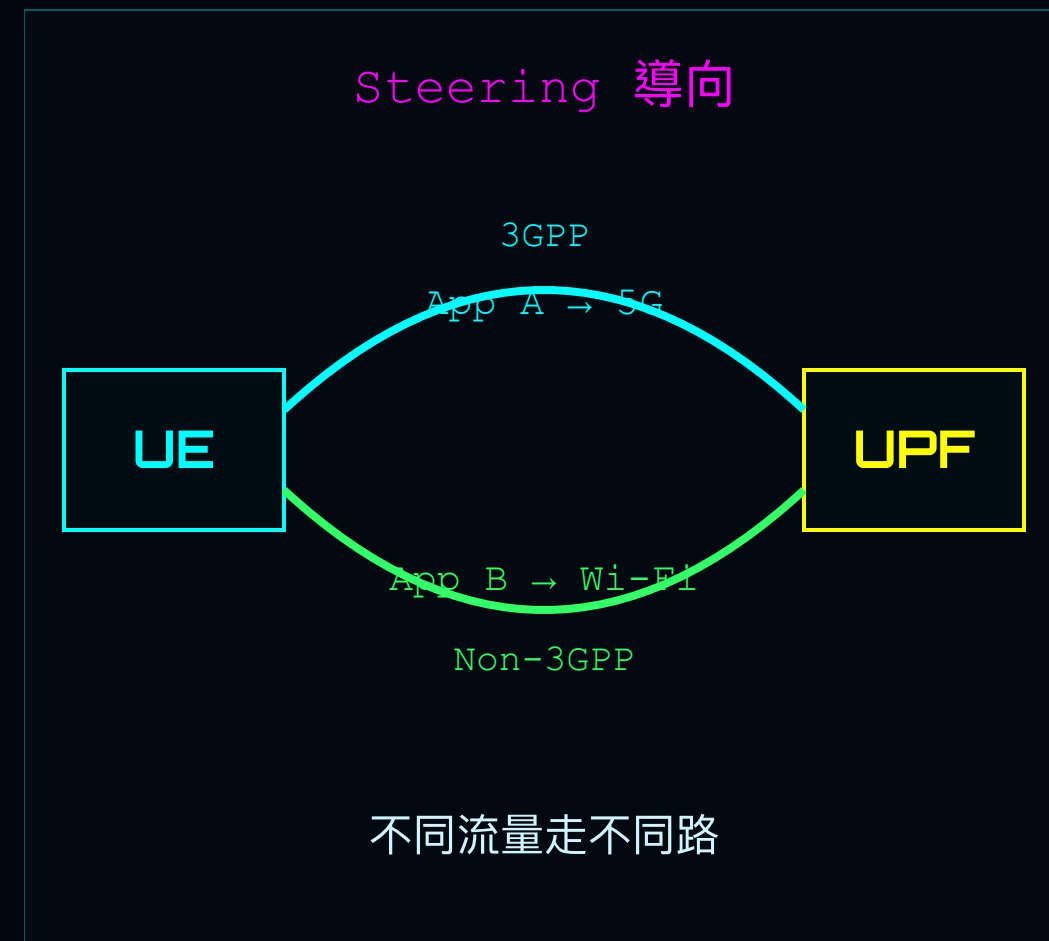


一支 UE、兩條路

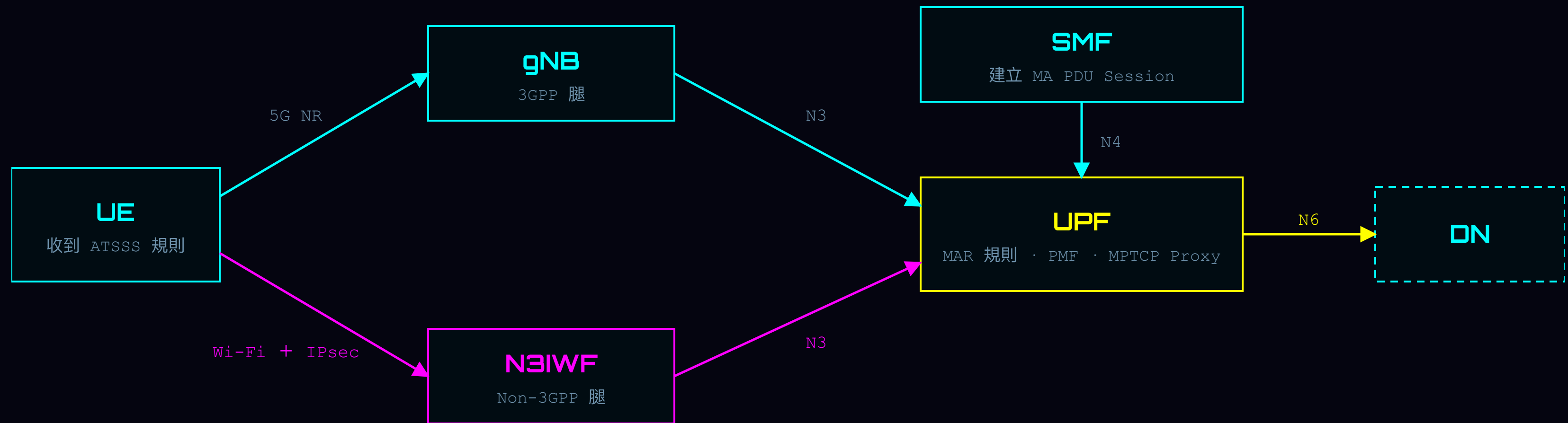
匯聚到同一個 UPF

UE 與核心網一起決定

三個 S



➤ MA PDU SESSION



一個 MA PDU Session，兩條使用者面的「腿」

➤ 怎麼分？STEERING 功能與模式

功能	做法	模式	規則
MPTCP	TCP 流量拆成多條子流，UPF 當 Proxy	Active-Standby	主路徑壞了才切
ATSSS-LL	低層分流，任何流量都可用	Smallest Delay	選延遲最小的
PMF	UPF 量 RTT、掉包率	Load-Balancing	依比例分流
		Priority-based	先塞滿高優先

UE 依 ATSSS Rule 決定上行怎麼分；UPF 依 N4 的規則（MAR）決定下行怎麼分。

➤ 誰負責什麼？

UE

多通道與分類

支援兩種接入、依 ATSSS Rule 分配上行流量（需要特定 UE 堆疊）

PCF

給策略

依應用類型、QoS 決定該用哪條路、什麼模式

SMF

建 MA PDU Session

產生 ATSSS Rule 給 UE、N4 規則給 UPF

UPF

執行與量測

下行分流、MPTCP Proxy、PMF 量測路況

➤ FREE5GC 的 ATSSS 實驗

1

5G NR → gNB

一條 3GPP 路徑

2

Wi-Fi → N3IWF (IPsec)

一條非 3GPP 路徑

3

兩條路匯聚到同一個 UPF

核心網依策略導向、切換或分流

社群展示過 N3IWF + 3GPP 的雙連線範例，是體驗「多接取、多路徑」很好的實驗平台。

➤ PART B 小結

非 3GPP AN + 閘道，對 5GC 來說就是另一種 RAN (N2 / N3)

N3IWF：不信任 Wi-Fi，用 IPsec / IKEv2 + EAP-5G 自己加密到底

TNGF：信任 Wi-Fi，用 802.1X 做接入認證，AP 與 TNGF 合作

TWIF：替不會講 NAS 的 Wi-Fi 裝置代辦 5GC 程序，私有 5G 的關鍵

不論哪種，身分仍由 5G-AKA / EAP-AKA' 決定 (AUSF / UDM)

ATSSS：MA PDU Session 同時用兩條路，Steering / Switching / Splitting

➤ 本週小結

AMF / SMF / UPF 之外，NRF、AUSF、UDM、UDR、PCF、CHF、NSSF、NEF 各司其職

free5GC 還實作了 SCP（轉送代理）與 BSF（PCF 綁定），都用 run.sh 參數開啟

非 3GPP 接入讓 Wi-Fi 也能共用同一套 5GC

理解它們，才能把 5GC 當成完整、可擴展的系統來思考

下一章：free5GC 部署實戰