



La sécurité dans les nouvelles générations de réseaux

Guy Pujolle

Guy.Pujolle@lip6.fr



Les réseaux : où en est-on?

Age de pierre

Age de bronze

Age de fer

2,5 M années

8000 années

3000 années

Imprimerie

Age de pierre

Age de bronze

Age de fer

1440

1850

1930

Internet

Age de pierre

Age de bronze

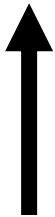
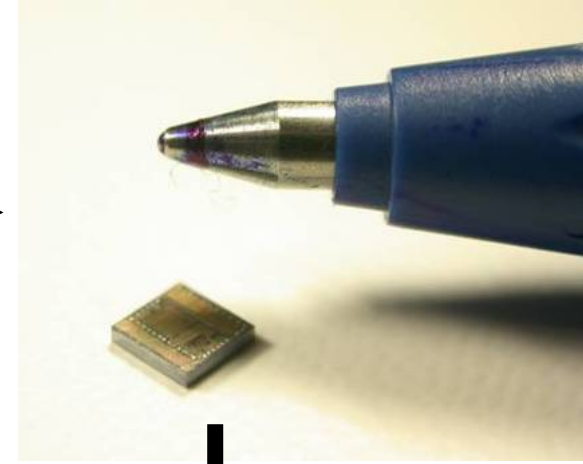
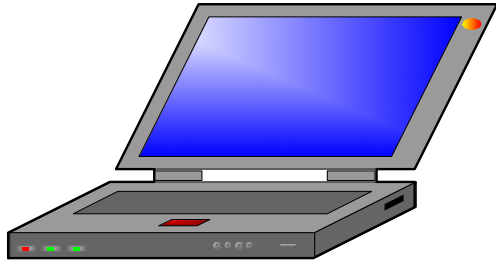
Age de fer

1970

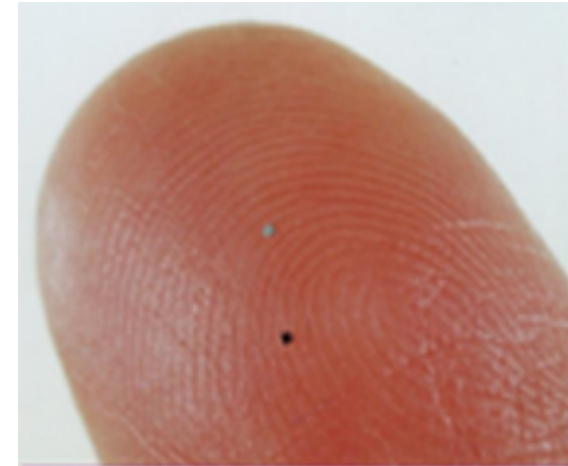
2010

2030

Évolution des réseaux



**Internet
Protocol**



Age

- **Age de pierre 2010 – Internet: de très nombreuses rustines ont été ajoutées**
- **Age de bronze 2010 - 2025 – Beyond IP: compatible avec IP**
- **Age de fer après 2025 – Post IP: non compatible avec IP**

Les réseaux sans fil

Les réseaux de mobiles

Rupture
technologique

GSM
GPRS
EDGE

UMTS
HSDPA
etc.

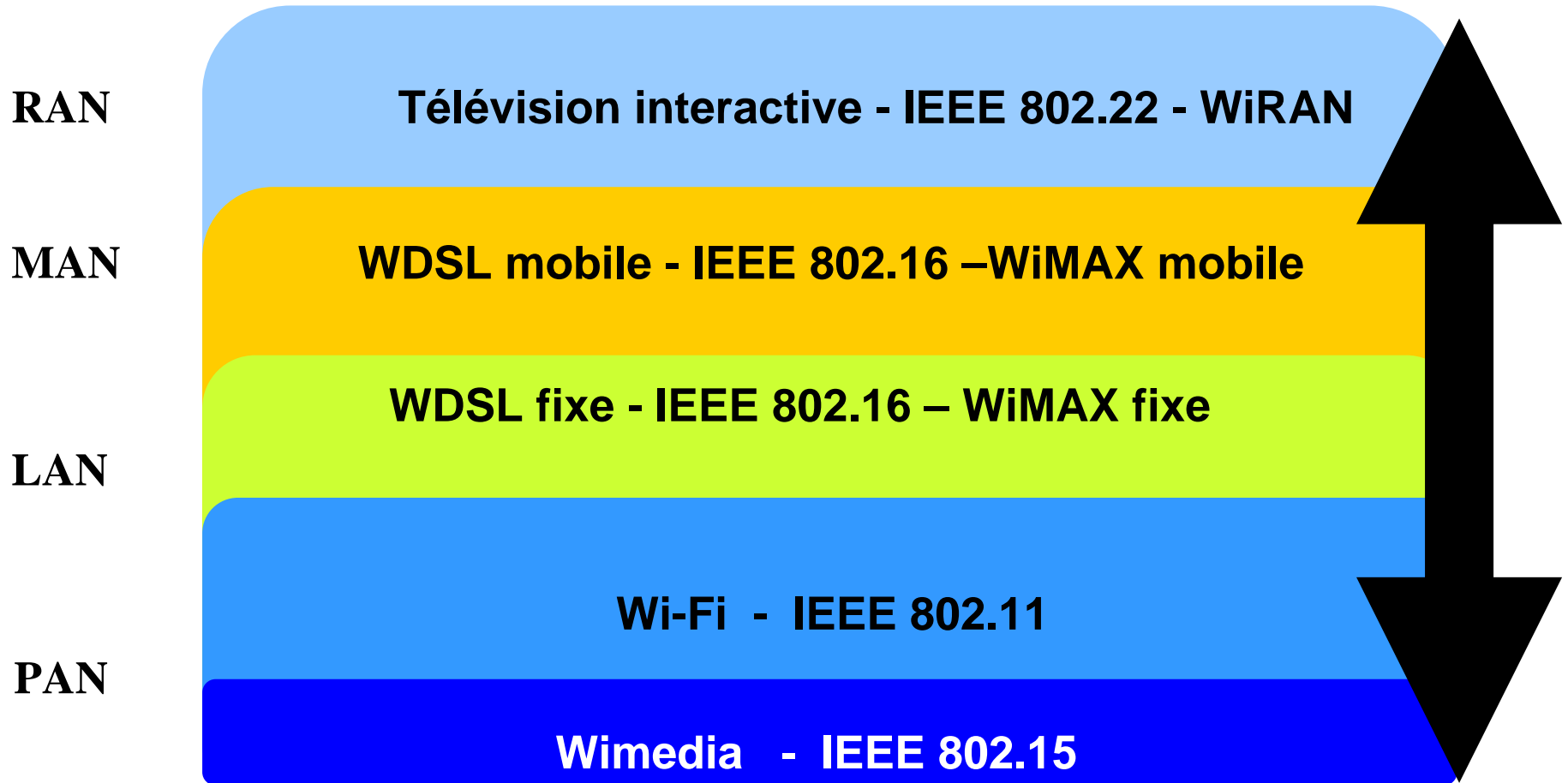
IS95
Cdma2000

3GPP2
EV DO

Wi-xx
+ IEEE 802.21

La gamme Wi-xx

Réseau IP - Ethernet



Standard pour les réseaux sans fil

● PAN

■ IEEE 802.15 et WiMedia

- IEEE 802.15.1 - Bluetooth
- IEEE 802.15.3 – UWB (Ultra Wide Band)
- IEEE 802.15.4 – ZigBee

● WLAN

■ IEEE 802.11 et Wi-Fi

- IEEE 802.11b, a, g
- IEEE 802.11n
- IEEE 802.11s

● WMAN

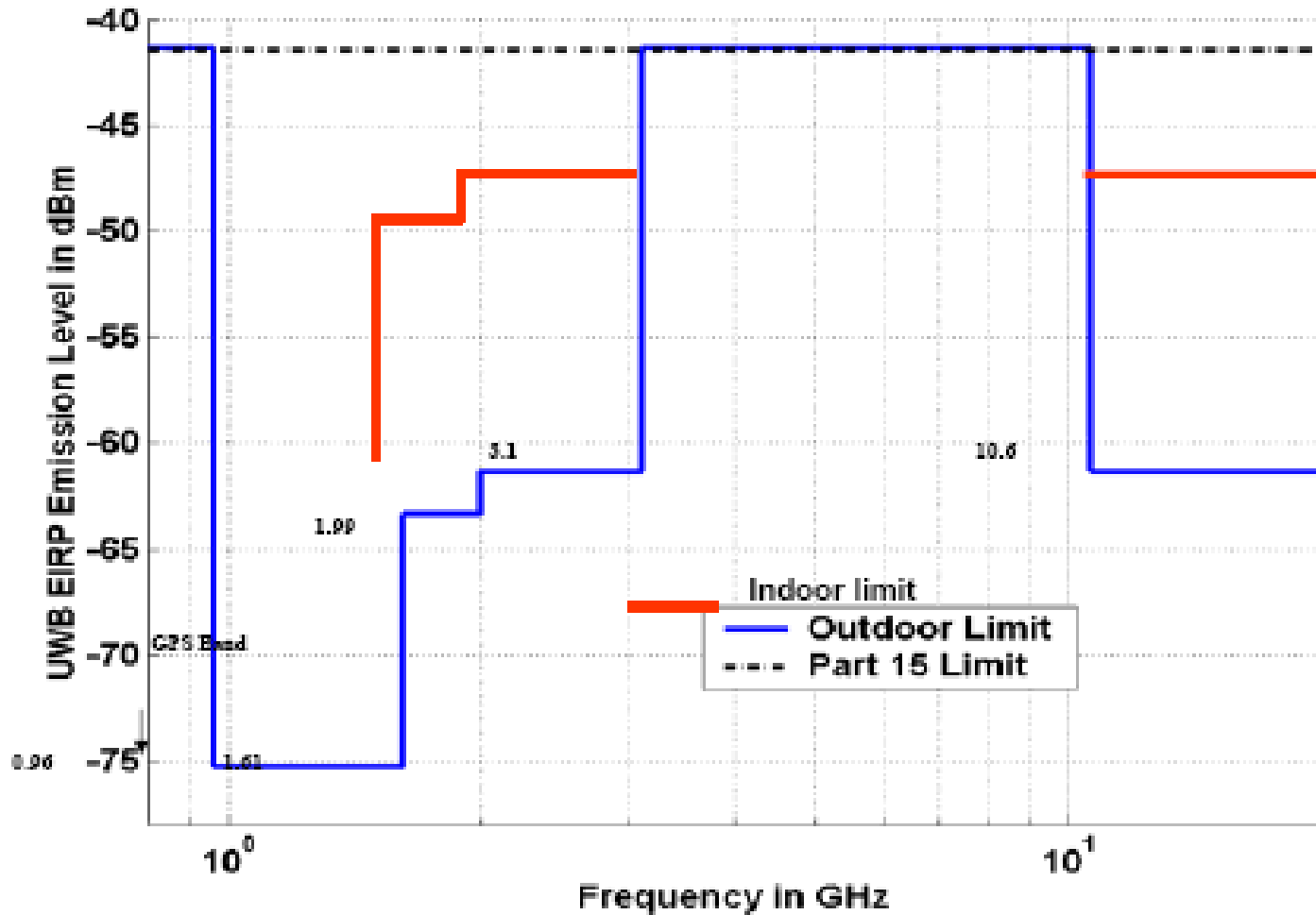
■ IEEE 802.16 et WiMax

- IEEE 802.16-2004
- IEEE 802.16e/IEEE 802.20 (WiMax Mobile)

● WRAN

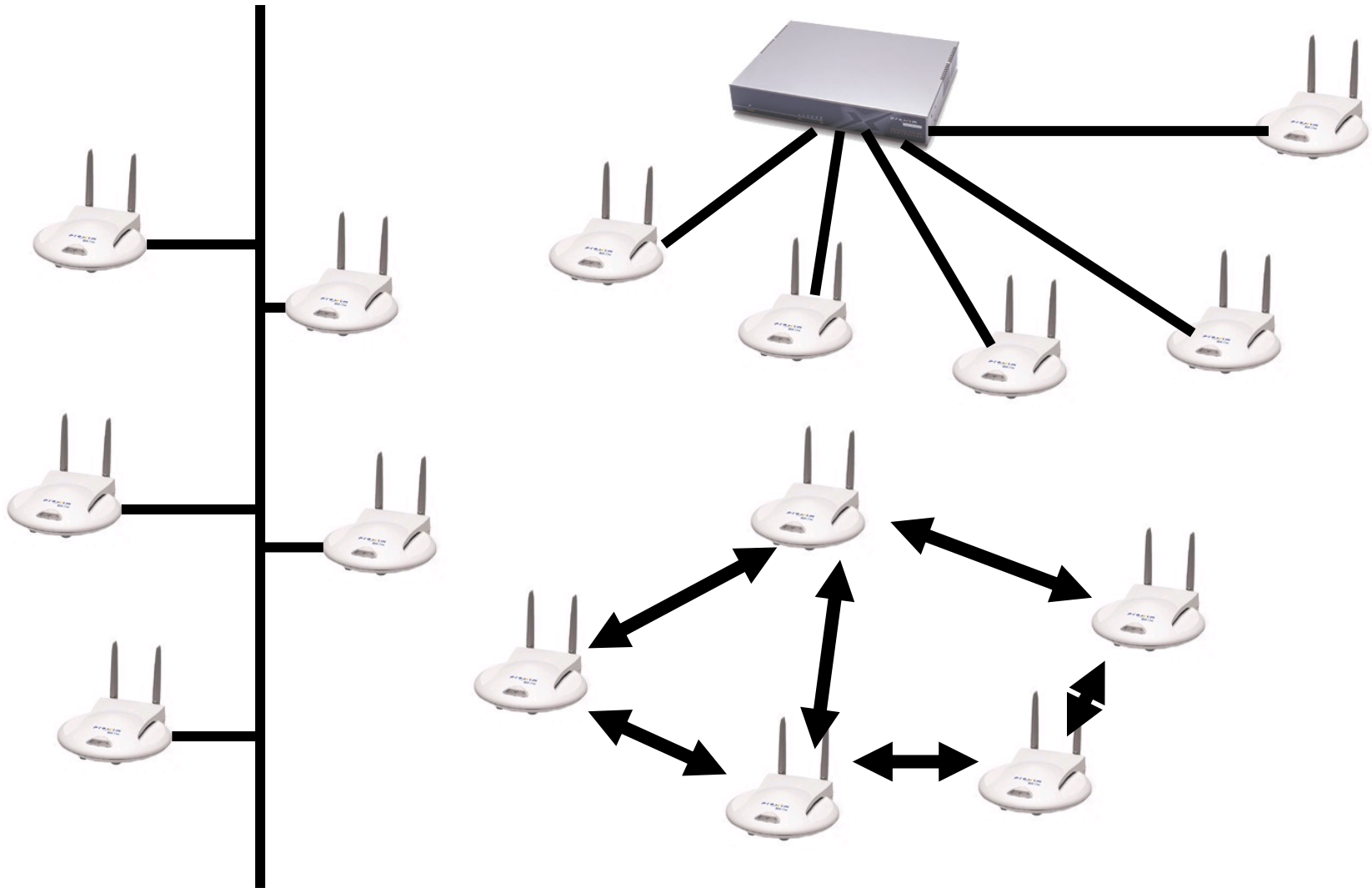
■ IEEE 802.22 et WiRAN

- Utilisation des bandes TV 54-862

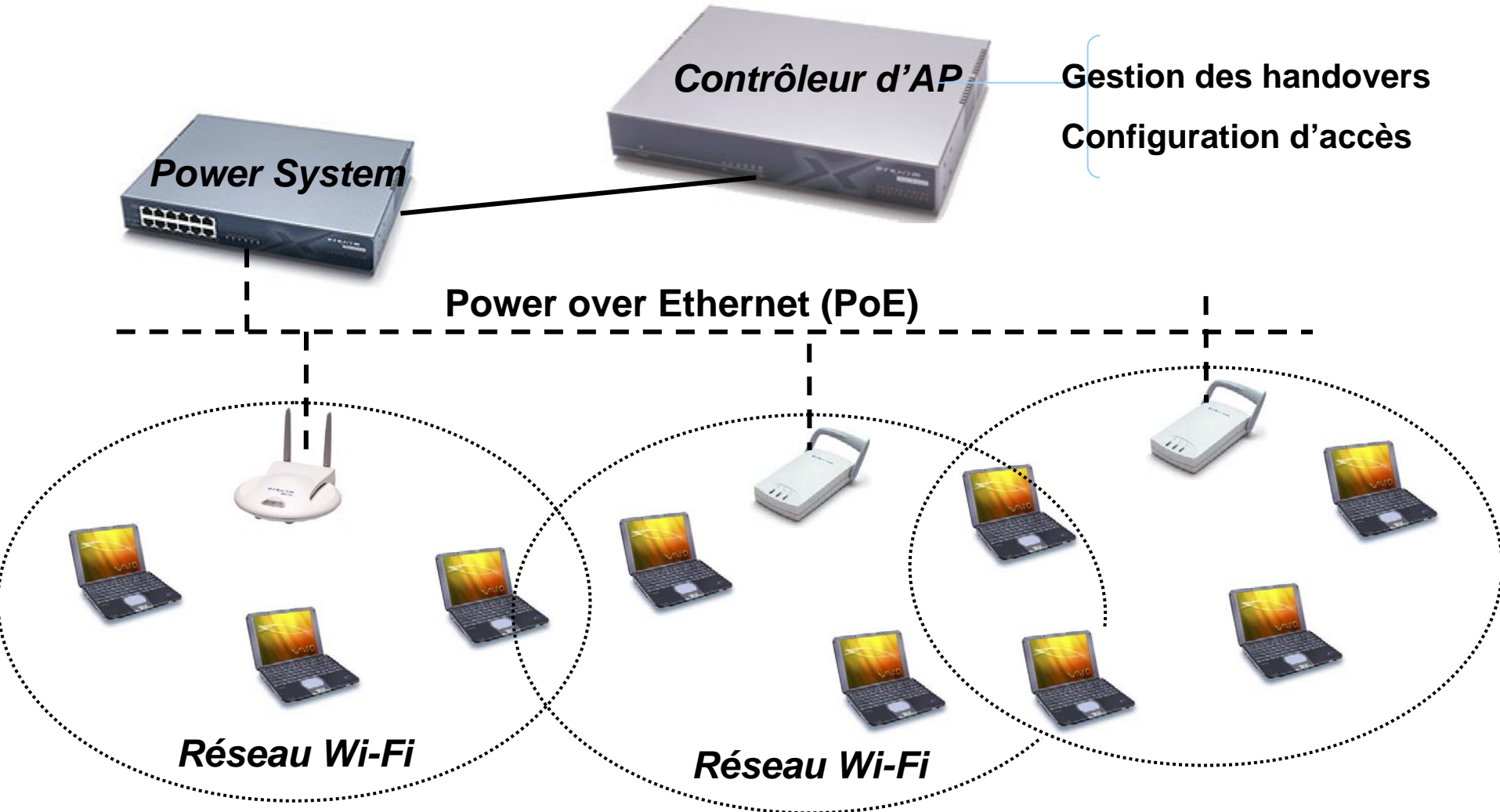


- **Control And Provisionning of Wireless Access Point**
- **Trois architectures de type Wi-Fi**
 - Les architectures de WLAN autonomes (Autonomous WLAN Architecture)
 - Les architectures de WLAN centralisées (Centralized WLAN Architecture)
 - Les architectures de WLAN distribuées (Distributed WLAN Architecture)

Wi-Fi

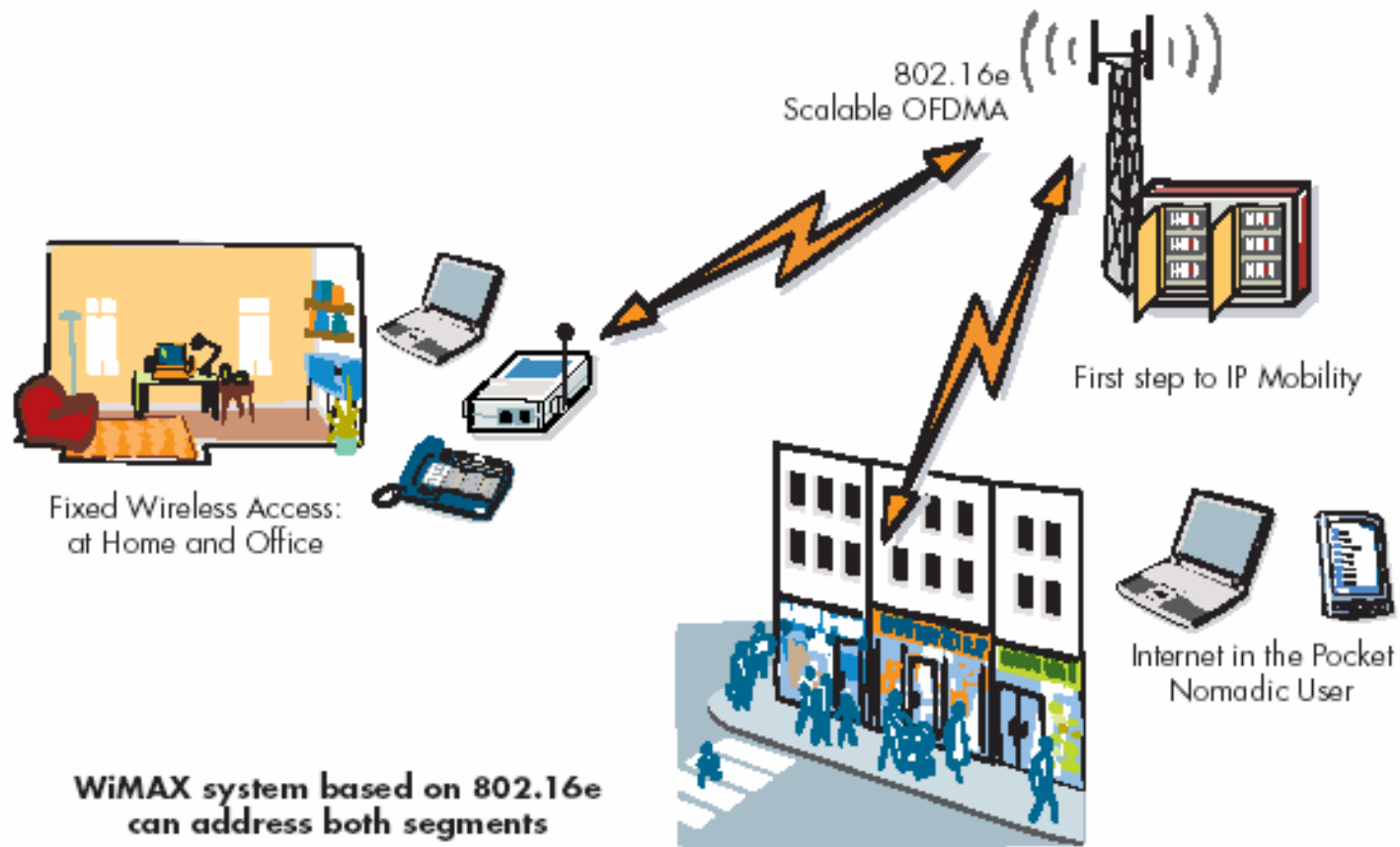


Réseaux Wi-Fi



IEEE 802.16 - WiMAX

WiMAX



OFDMA: Orthogonal Frequency Division Multiple Access

IEEE 802.16

- **IEEE 802.16-2004**

- **IEEE 802.16e-2005**

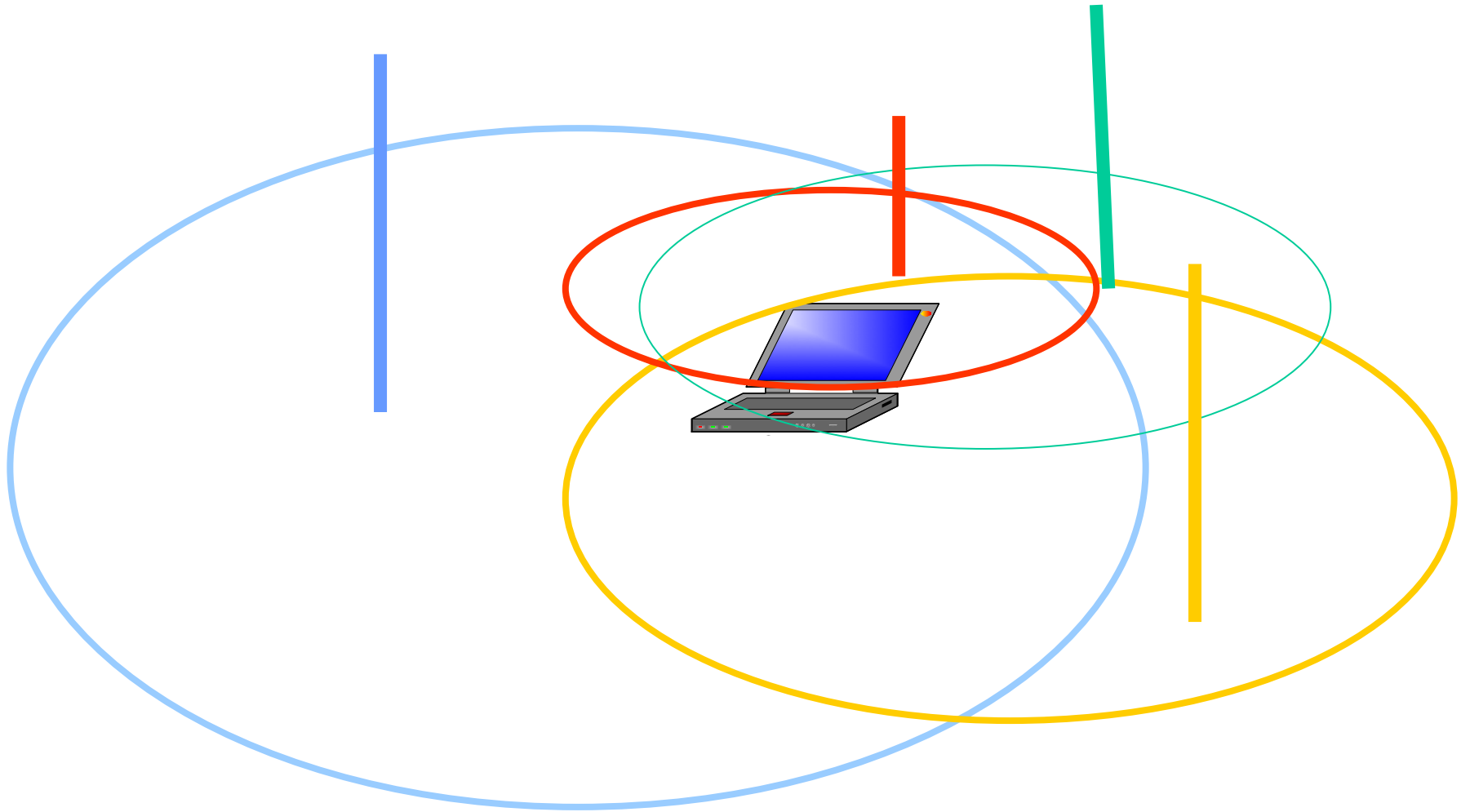
- **Produit Intel**

- Le processeur Rosedale
- Le processeur Centrino n

- WiFi-WiMAX
- WiFi- WiMAX-Wimedia
- WiFi-WiMAX-Wimedia multi-homé



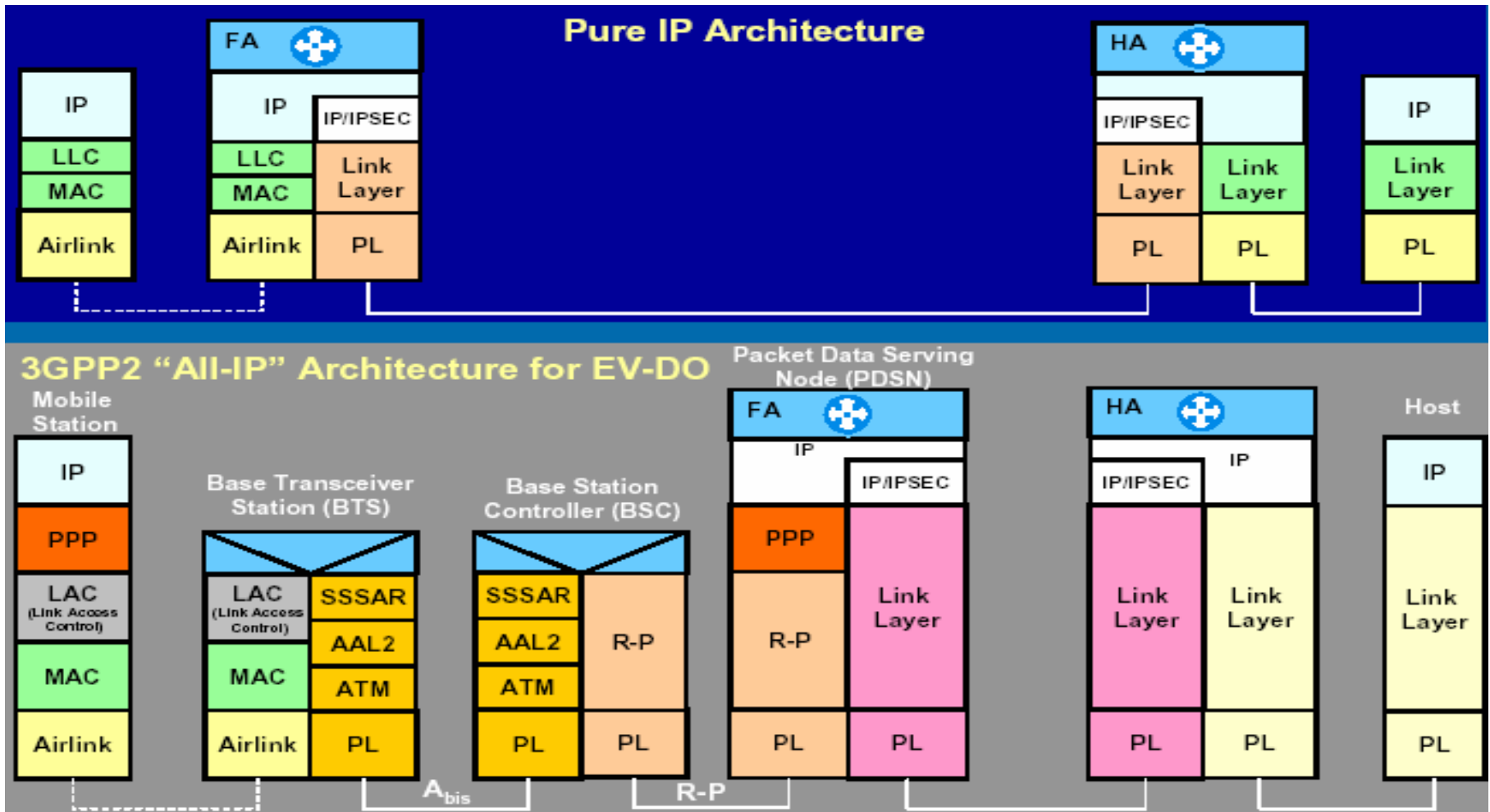
Multi-technologies and multi-homing



● Nouvelle spécification pour Universal WiMax

- Fréquence < 3.5 GHz
- Au moins 1 Mbit/s par utilisateur
- Vitesse jusqu'à 130 km/h
- Grande cellule (1 km approximativement)
- Ambient
- Garantie de QoS
- Sécurité EAP-TLS

Architecture IEEE 802.16e vs 3GPP2



Source IEEE

WiRAN : 802.22

- **Bande de fréquence : 54 – 862 MHz**
 - France : SECAM sur la bande 47 – 798 MHz
 - Dividende numérique
- **Cognitive radio**
 - Terminaux sans licence mais ne perturbant pas les communications avec licence
- **Canaux de 6 ou 8 MHz**
 - Vitesse de transmission : 18 Mbit/s / canal de 6 MHz
 - Voie descendante 1,5 Mbit/s à 4 Mbit/s
 - Voie montante : 384 kbit/s ?
- **Puissance : 1 W descendant, 100 mW montant**
- **Technique de transmission**
 - OFDM
- **Support de la qualité de service au niveau MAC**
- **Coût très faible**

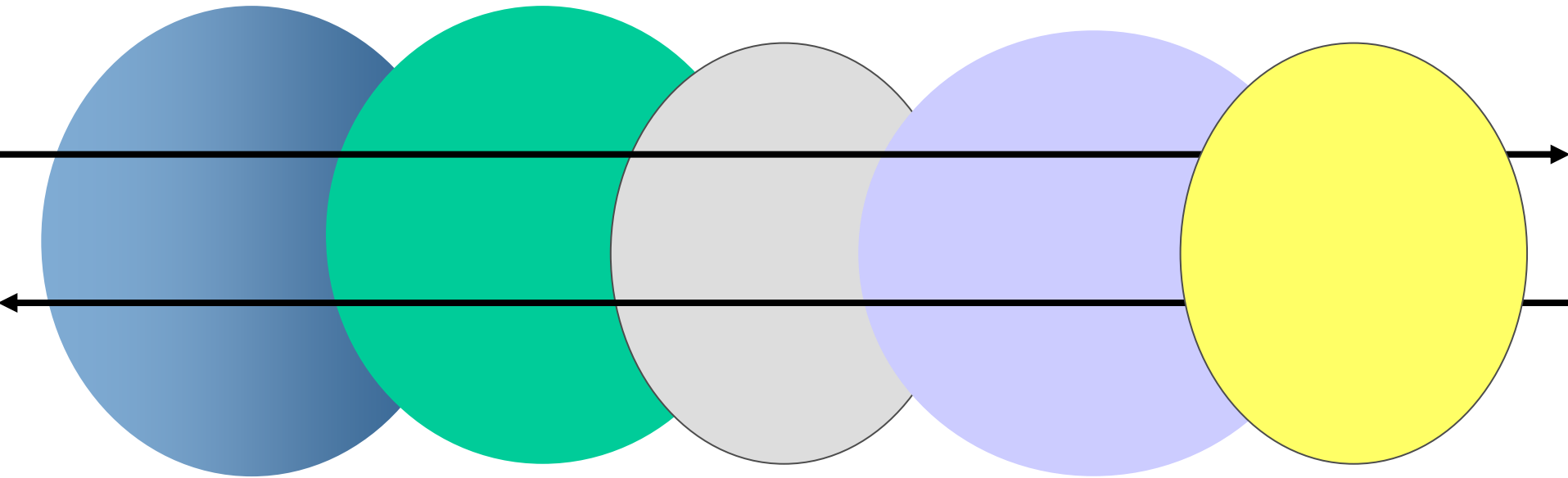
IEEE 802.22 (USA)

- **Le terminal n'a pas besoin d'être déclaré (aux USA)**
- **Les caractéristiques radio sont contrôlées par l'émetteur**
- **GPS/Galileo pour déterminer les fréquences à utiliser**
- **Couverture jusqu'à une cinquantaine de kilomètres**

- **300 MHz de bande passante**
 - 300 000 utilisateurs multimédias par point d'accès
 - 1 000 000 de paroles téléphoniques

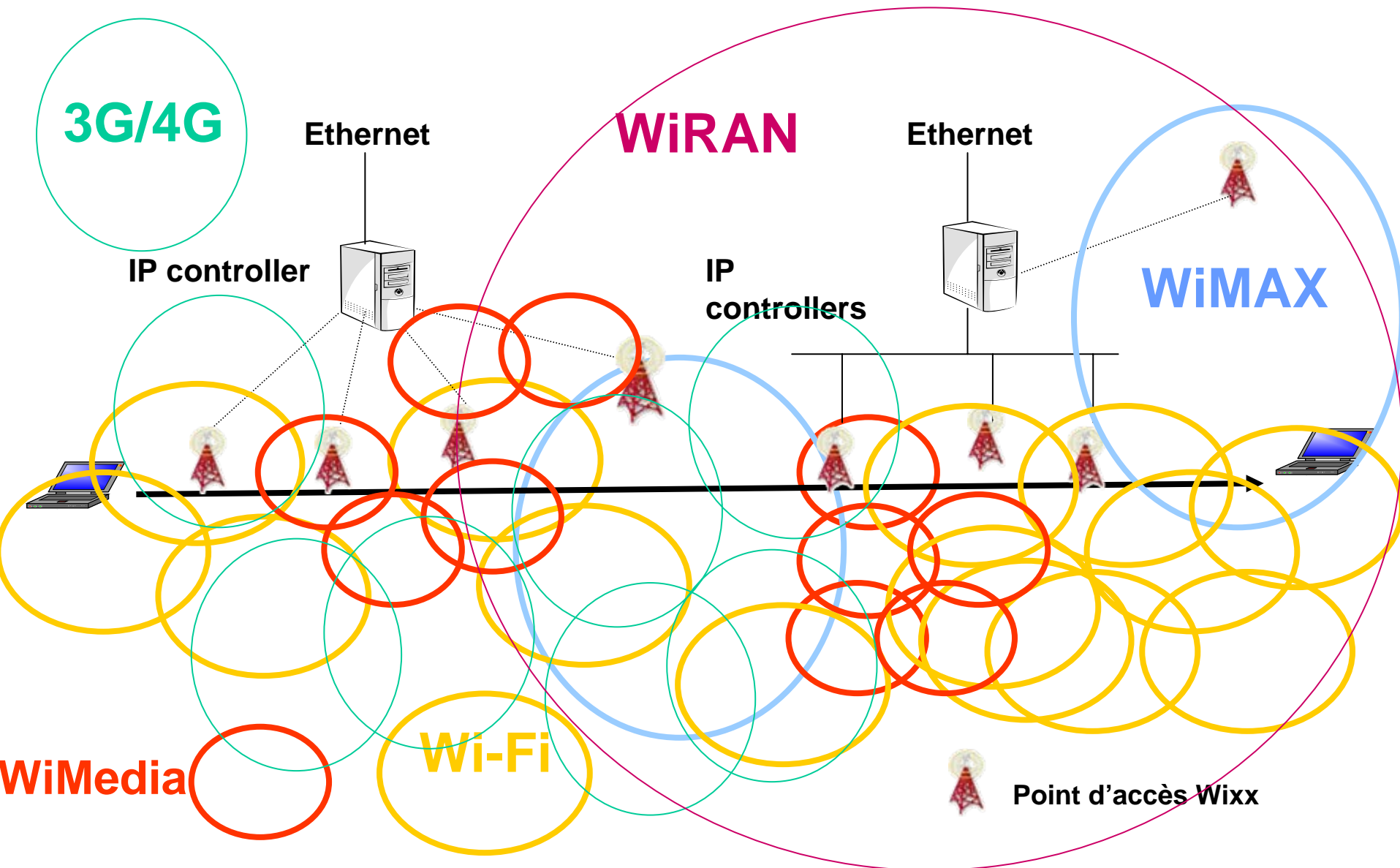
IEEE 802.21 Media Independent Handover Scheme

- Handover entre les différents standard 802 (802.15, 802.11, 802.16, 802.20, 802.22)



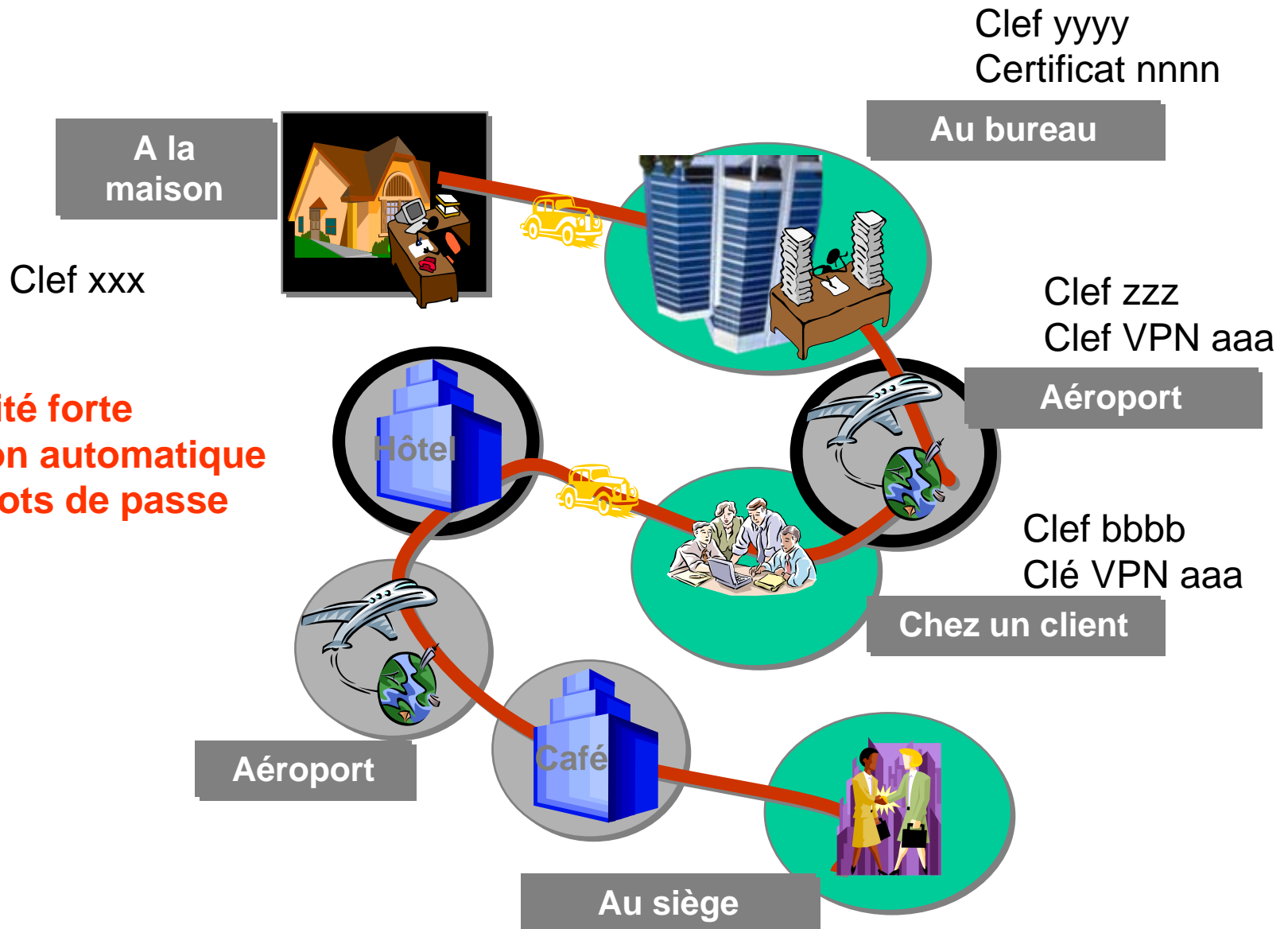
WiMedia, Wi-Fi, WiMAX, Wi-Mobile, WiRAN

L'Internet sans fil



La sécurité

Le nomadisme



Sécurité dans les hotspots

● Nouvelle loi sur la traçabilité : garder pendant 1 an de nombreuses données

- Selon le décret publié le 26 mars, il s'agit des informations permettant d'identifier un utilisateur. Soit :
 - Les données relatives aux équipements terminaux de communication (ordinateur...) utilisés.
 - Les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication.
 - Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.
 - Les données permettant d'identifier le ou les destinataires des communications électroniques



Une traçabilité fermée (uniquement sur requête judiciaire)
Respect des libertés individuelles

802.11 Sécurité

- **1er génération Wireless Equivalent Privacy (WEP), définie dans le standard 802.11**
- **2è génération , 802.1x architecture (with WEP)**
- **3è génération , TKIP, compatibilité matérielle avec WEP, WPA**
- **4è génération , 802.11i + AES, incompatibilité matériel avec WEP**

Sécurité Wi-Fi – 1^{er} génération

• Accès au réseau

- Service Set ID (SSID) : équivalent au nom de réseau
- Access Control List (ACL) : basé sur les adresses MAC

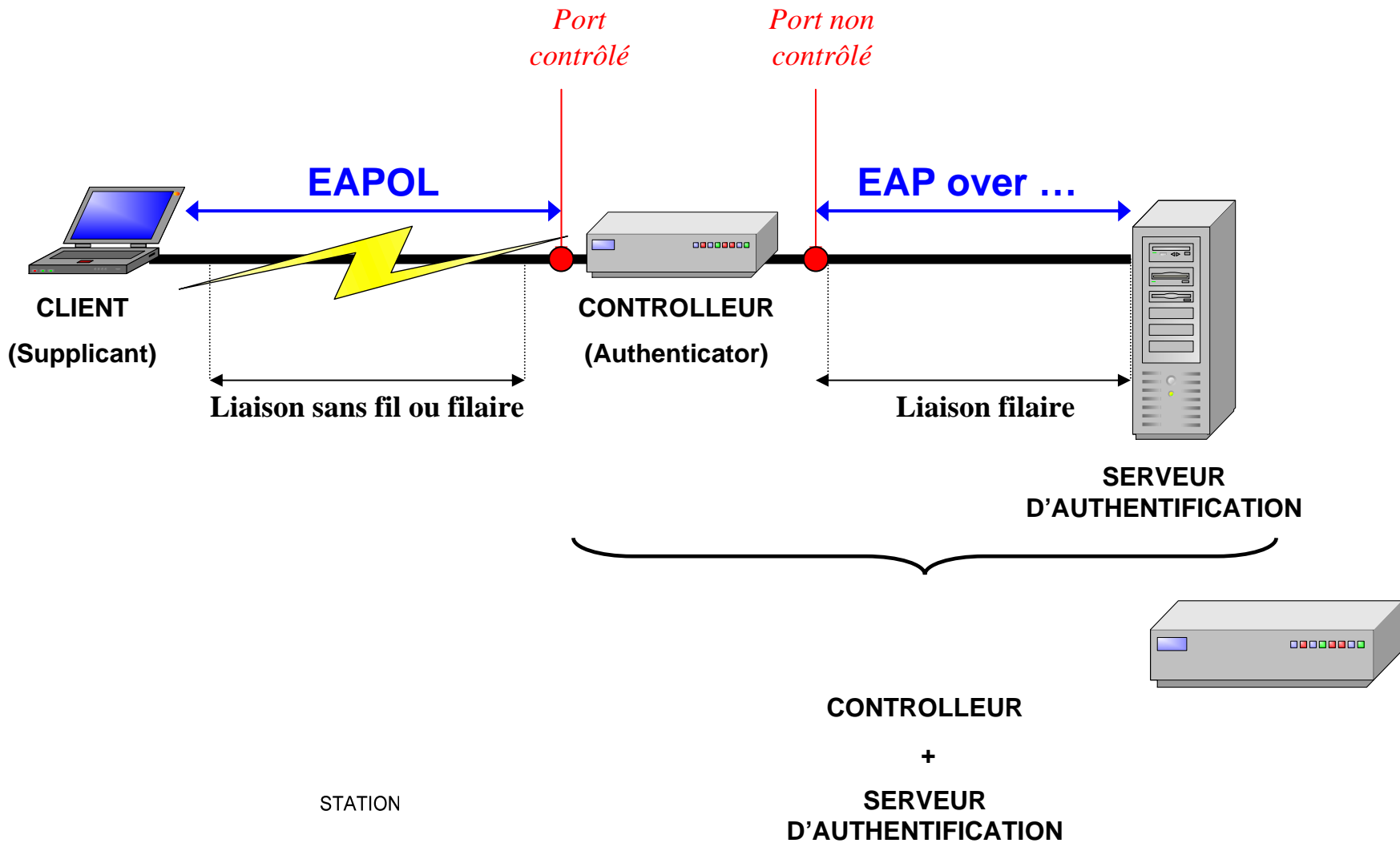
• Wired Equivalent Privacy (WEP) : Mécanisme de chiffrement fondé sur le RC4

- Authentification
- Chiffrement

Sécurité Wi-Fi – 2è génération

- **IEEE 802.1x est utilisé pour tous les réseaux IEEE 802.x**
- **Utilise le protocole Extensible Authentication Protocol (EAP)**
- **Utilisation d'un serveur d'authentification de type RADIUS : Remote Authentication Dial in User Service**
 - Protocole d'authentification client/serveur utilisé pour l'accès à distance

IEEE 802.1x



Sécurité Wi-Fi – 3^è génération

● **TKIP : Temporal Key Integrity Protocol**

- MIC (Message Integrity Code)
- Nouvelle implémentation de l'IV (Initialization Vector)
- Une nouvelle clef régulièrement
- Une gestion améliorée des clés

● **Inconvénient : performance si les changements de clef sont rapides**

Sécurité Wi-Fi – 3^è génération

● **WPA : Wi-Fi Protected Access**

- Initialisé par la Wi-Fi Alliance
- Fondé sur TKIP : changement de la clé régulièrement
- IEEE 802.1x

● **Sécurité assurée pour quelques années**

Sécurité Wi-Fi – 4^e génération

- **Juin 2004: WPA2**
- **Utilisation de TKIP et de 802.1x**
- **Nouvel algorithme de chiffrement : AES**
 - L'algorithme RC4 est remplacé par AES
 - AES nouveau standard pour le chiffrement des données
 - Algorithme très fiable et rapide

Autres solutions pour la sécurité

Autres solutions

■ Carte à puce

- ➔ Sécurisation des clés de chiffrement et des certificats
- ➔ Algorithme dans la carte à puce

■ Firewall/Filtre applicatif

- ➔ Filtre sur les ports
- ➔ Filtres applicatifs
- ➔ Détection des applications avec port dynamique

■ VPN

Normalisation future

■ Biométrie

Filtres applicatifs

- **Le firewall permette de bloquer des applications en fonction du n° de port**
 - De nombreuses applications utilisent des ports dynamiques (exemple : P2P)
- **Le filtre applicatif se base sur la sémantique des flots**
 - Reconnaissance de la grammaire du protocole
 - Adéquation avec le RFC

Réseaux Privés Virtuels (VPN)

- **But : créer un « tunnel » sécurisé entre un client et un serveur**
- **Le VPN permet :**
 - D'identifier les clients
 - D'autoriser les clients
 - De chiffrer le trafic des clients
- **IPSec (Internet Protocol Security)**
 - PPTP
 - L2TP

Les nouveaux réseaux Wi-xx

● Arrivée des réseaux Wi-xx (Wi-Fi, WIMAX mobile, etc.)

- Ce sont des réseaux IP natifs

● Solution

- Sécurisation avec l'équivalent de la carte SIM dans le monde IP: la carte EAP-TLS



Les solutions

● TPM (Trusted Platform Module)

- Trusted Computing Group (TCG)
- Améliorer la sécurité des plates-formes
- Solution fixe

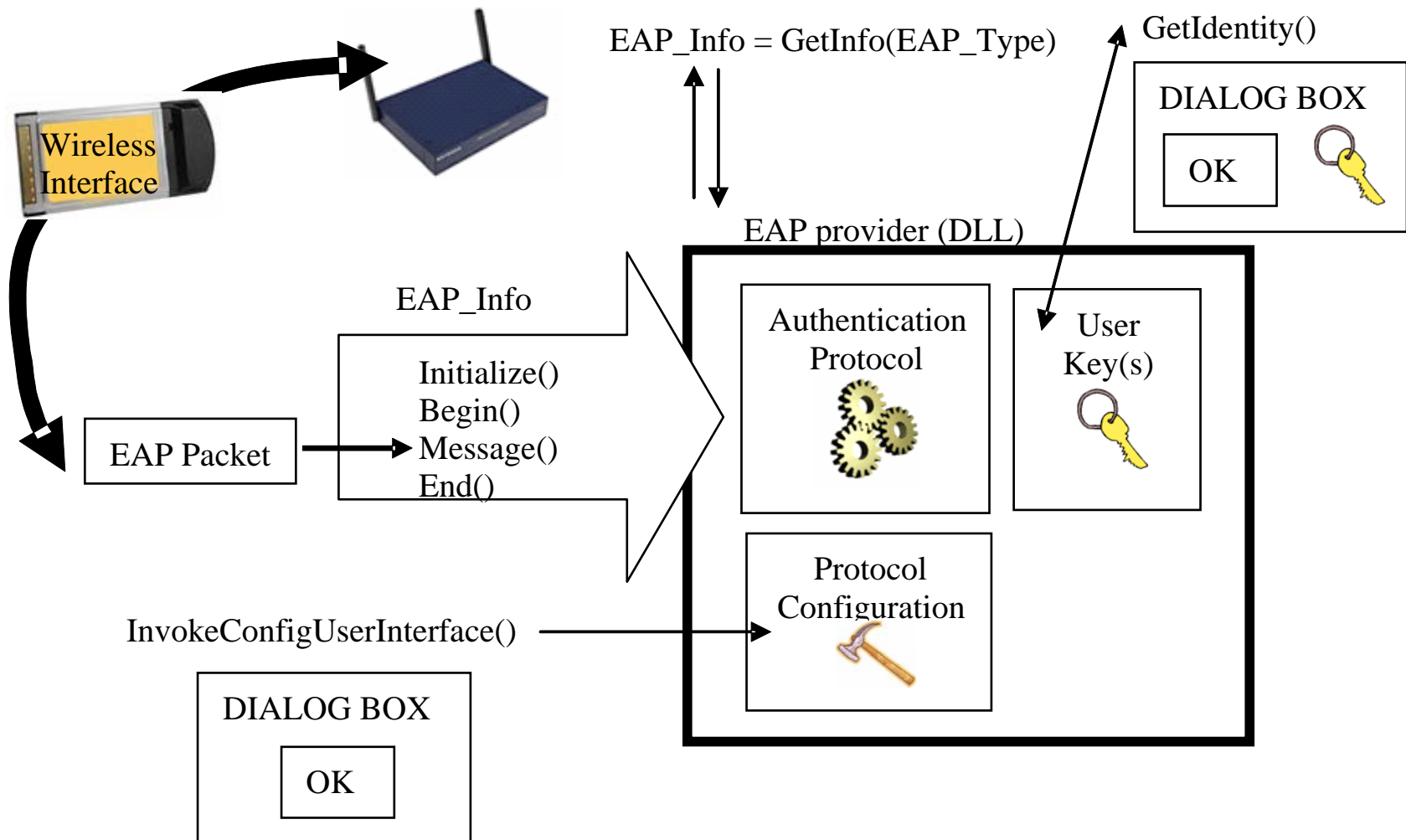


● TEAPM (Trusted EAP Module)

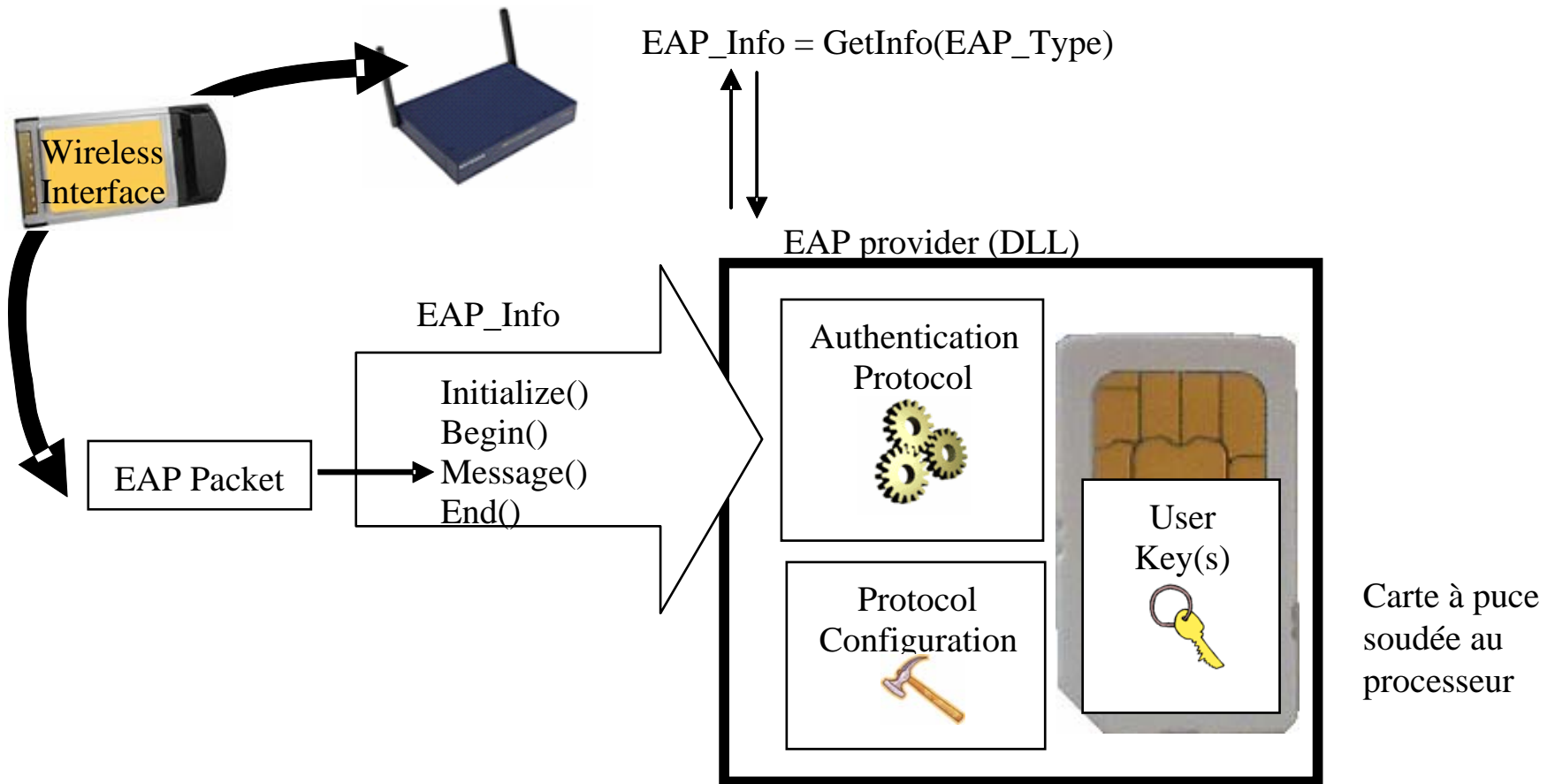
- Solution pour mobile



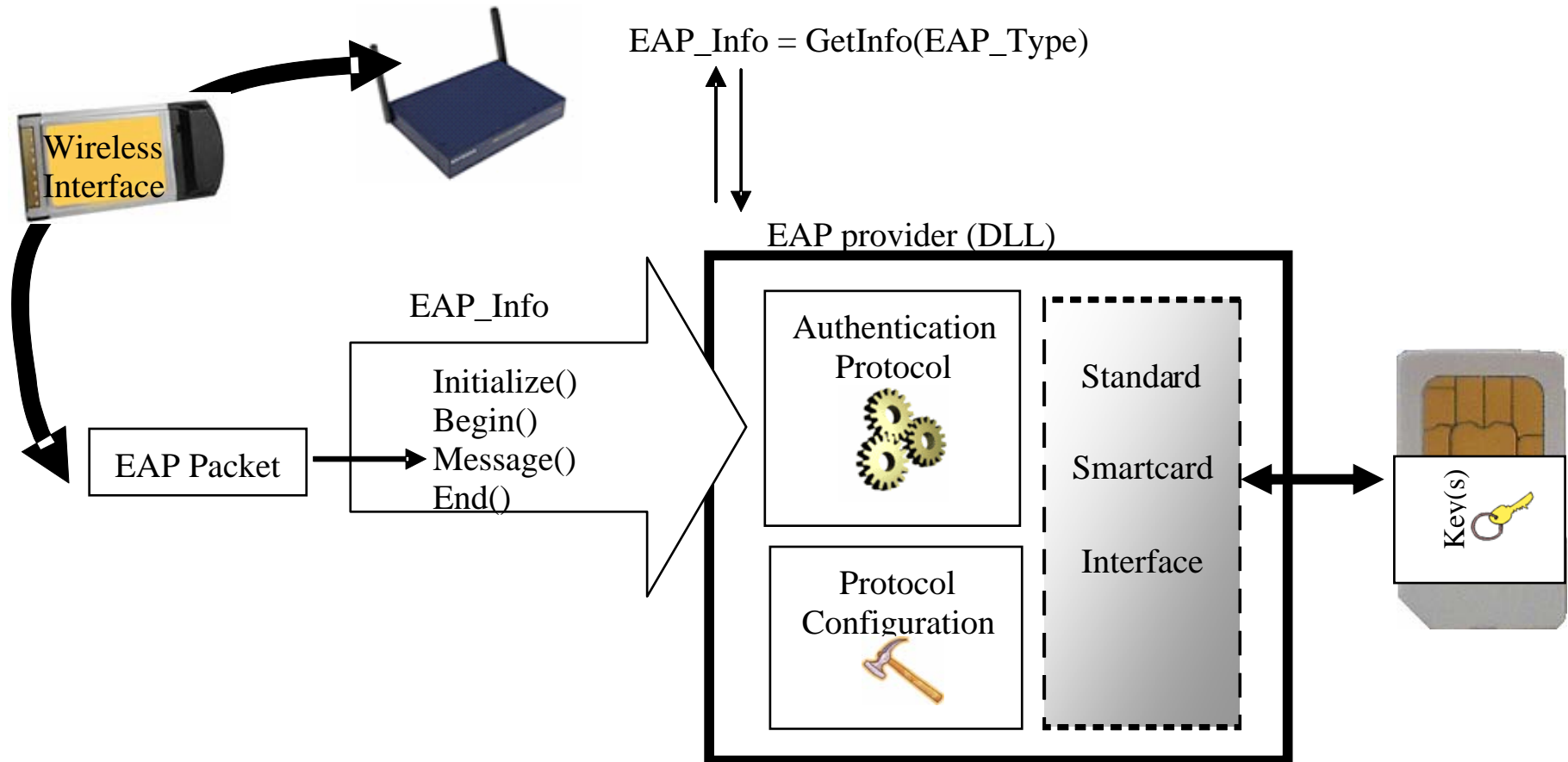
Cas classique



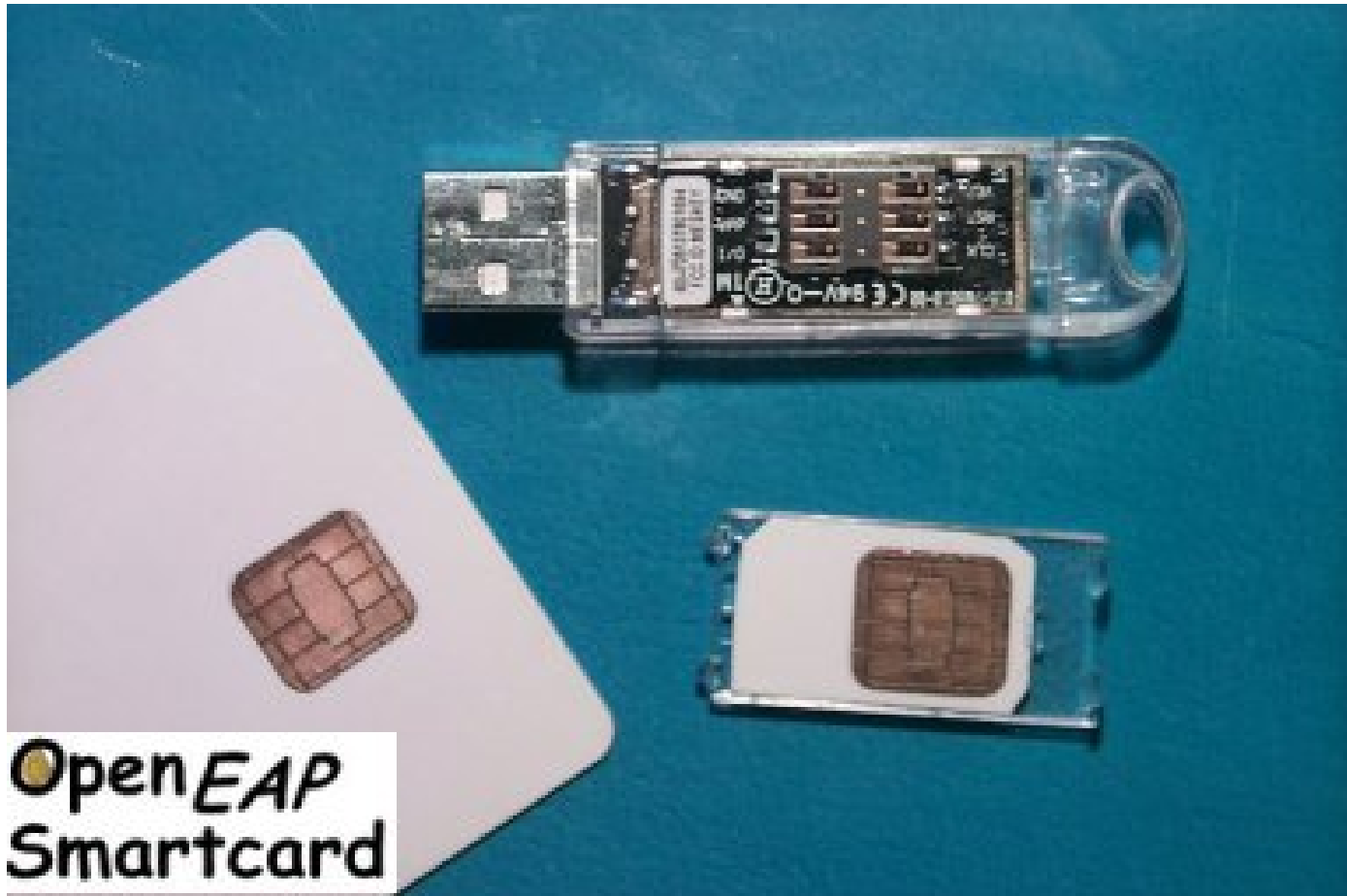
TPM Trusted Platform Module



TEAPM Trusted EAP Module



Open EAP Smartcard



Traçabilité

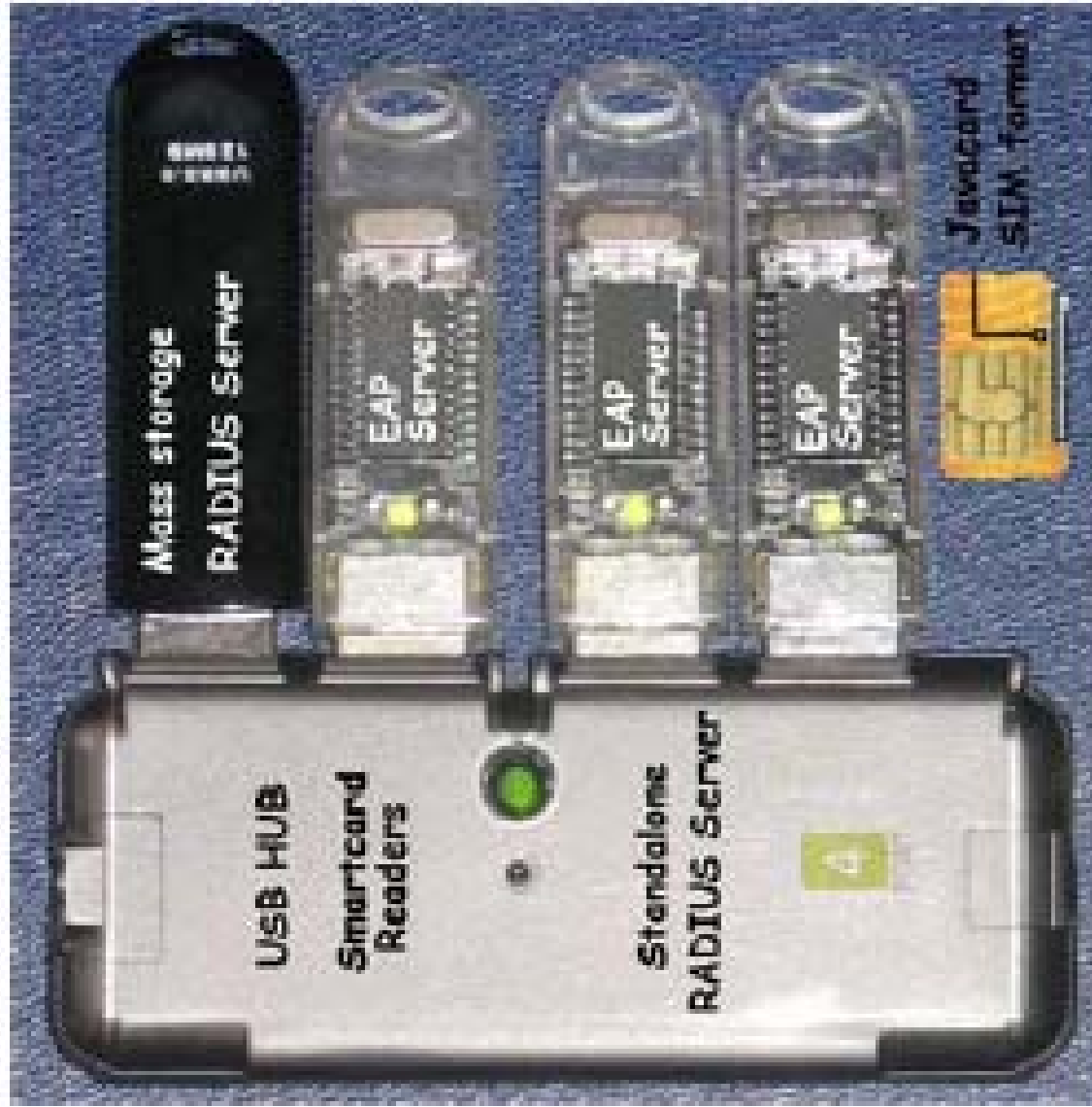
• Traçabilité ouverte

- Le responsable du cybercafé peut connaître les identifications

• Traçabilité fermée

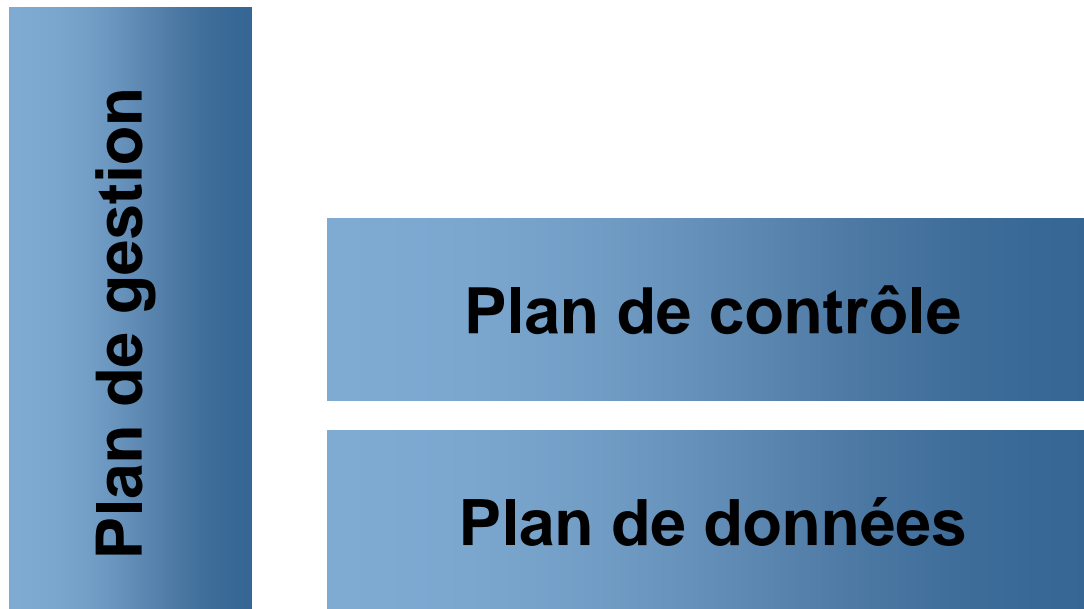
- Les états/organisations exigent de plus en plus la traçabilité des échanges d'information. Les citoyens souhaitent garder l'anonymat sur les réseaux (privacy).
- La technologie de protection d'identité concilie traçabilité et respect de la vie privée.

Serveur d'authentification

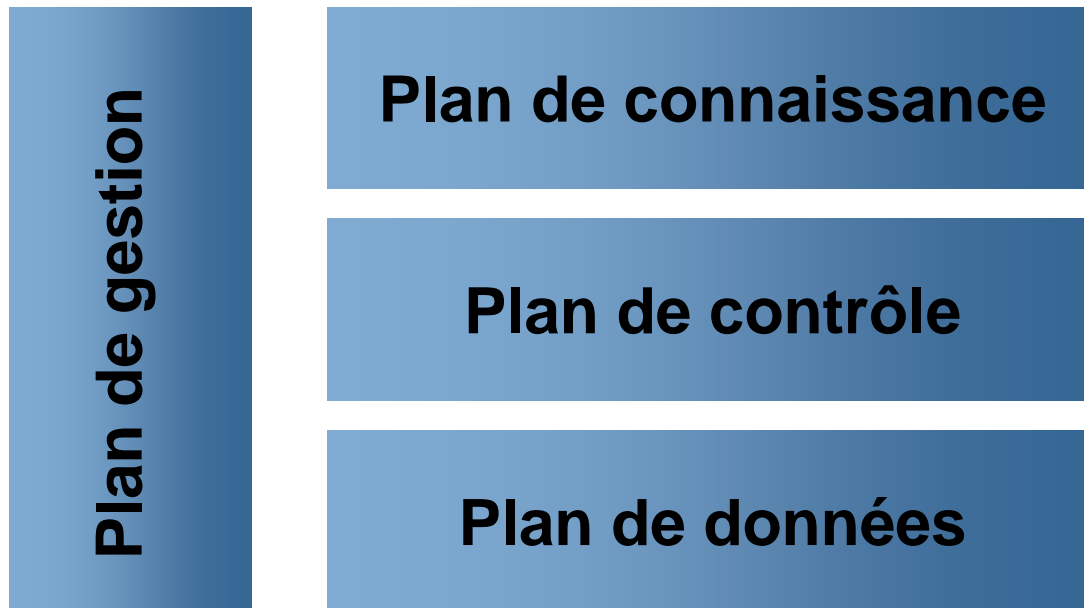


*Réseaux « **autonomic** »*

Architecture classique



Plan de connaissance



Le plan de connaissance

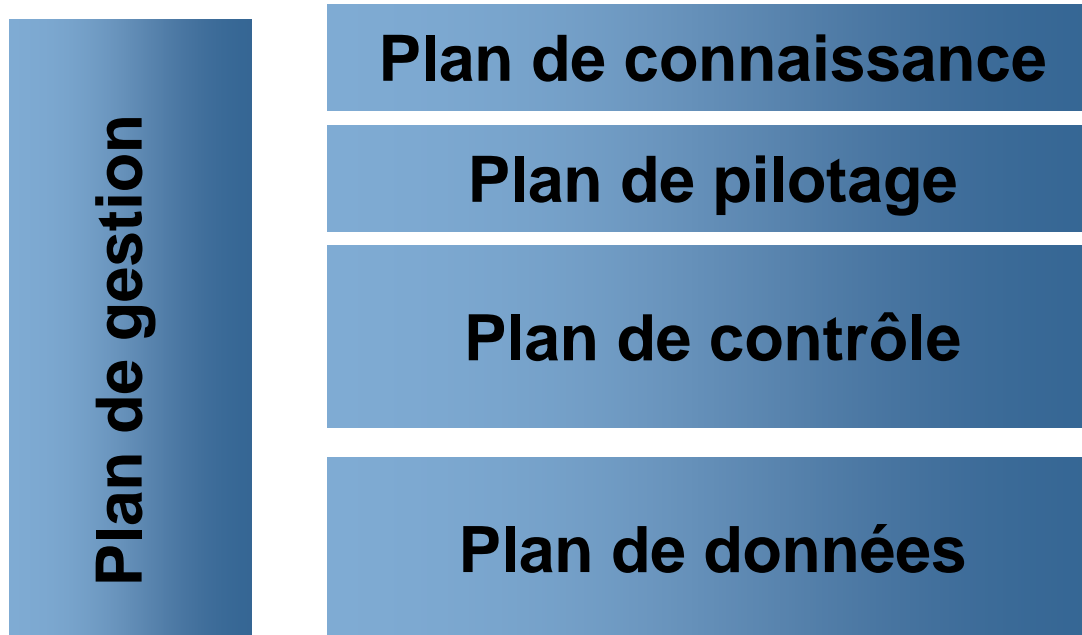
● Les réseaux « autonomes » possèdent un plan de connaissance

- Rassemble les connaissances du réseau
- Chaque point a une vue située du réseau

● Une intelligence est nécessaire pour piloter le réseau

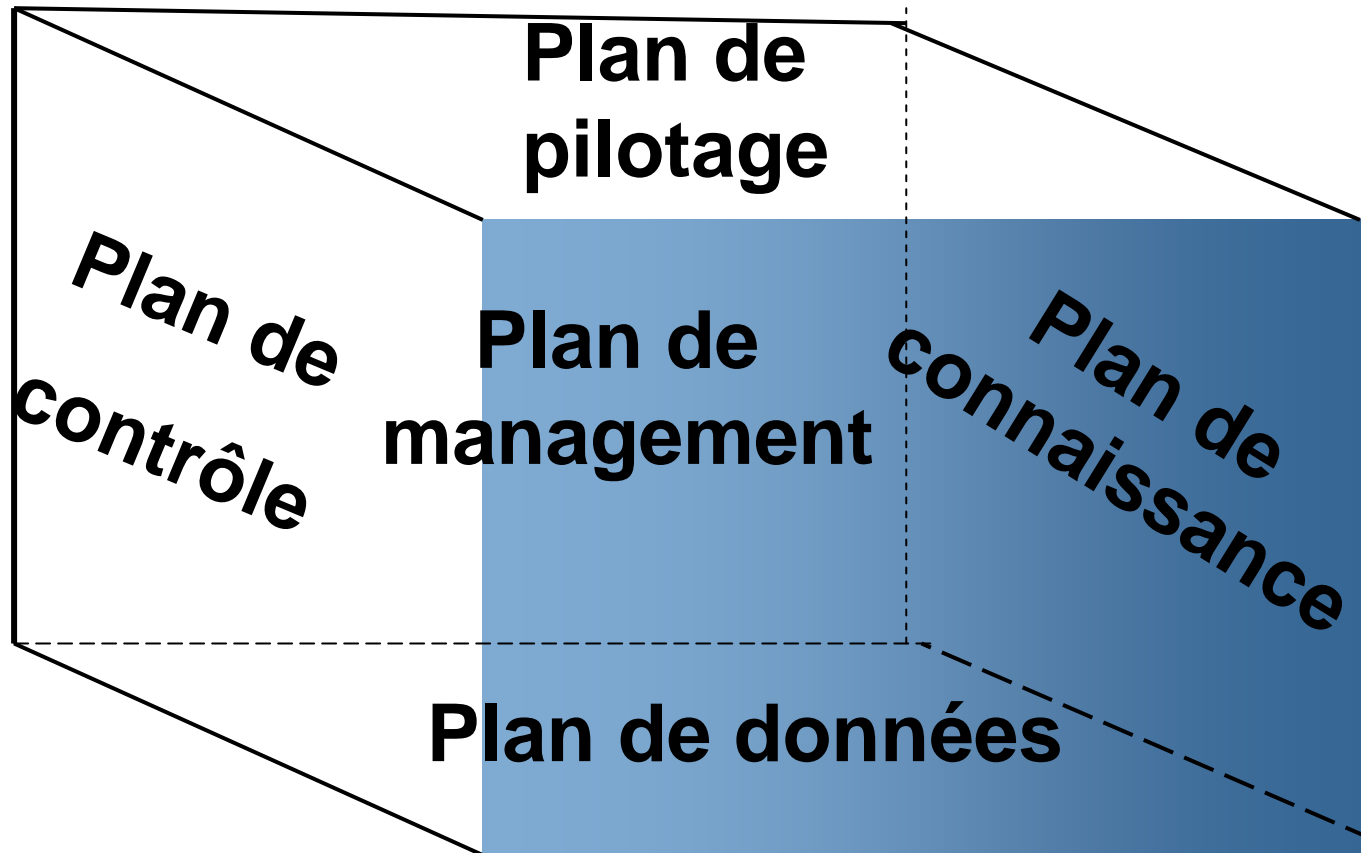
- Comprendre le comportement du réseau
- Accède à différentes informations et à des composants gérant la connaissance

Plan de pilotage

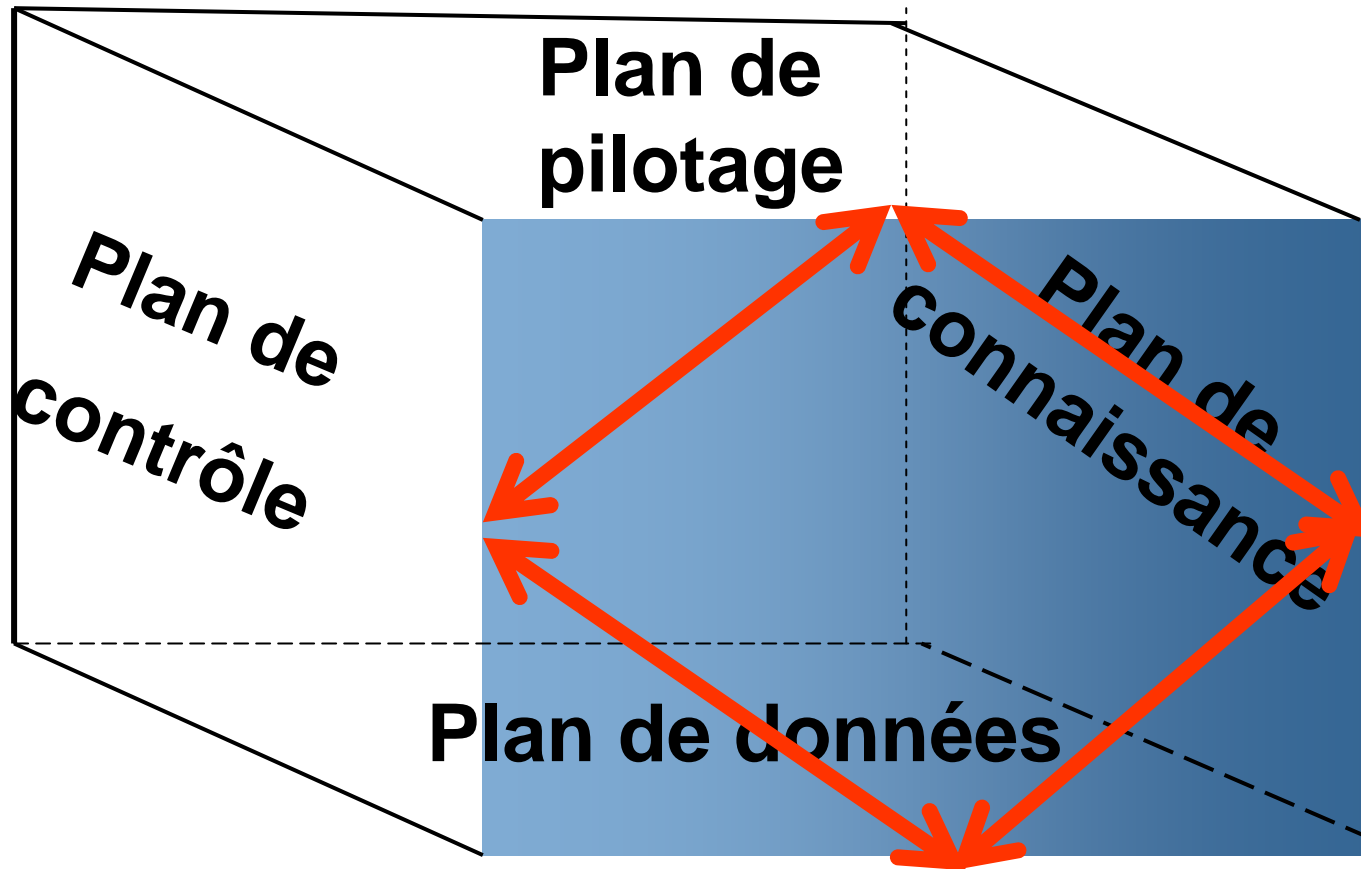


Le plan de pilotage possède les algorithmes de pilotage du réseau

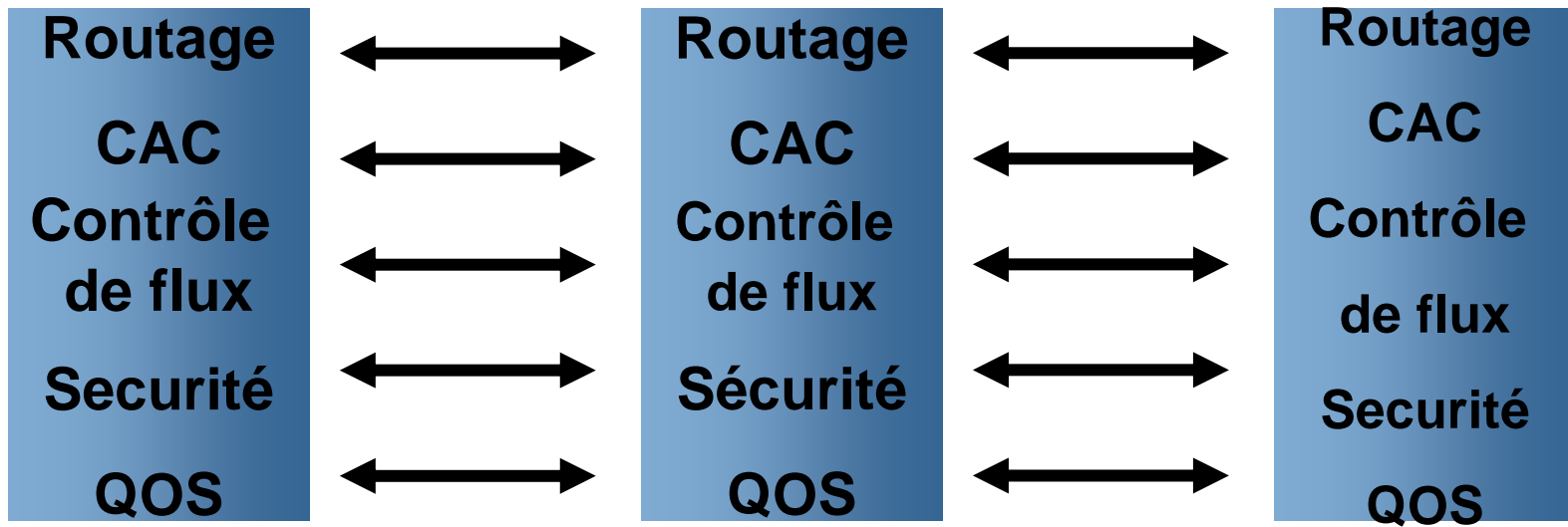
Réseau “autonomic”



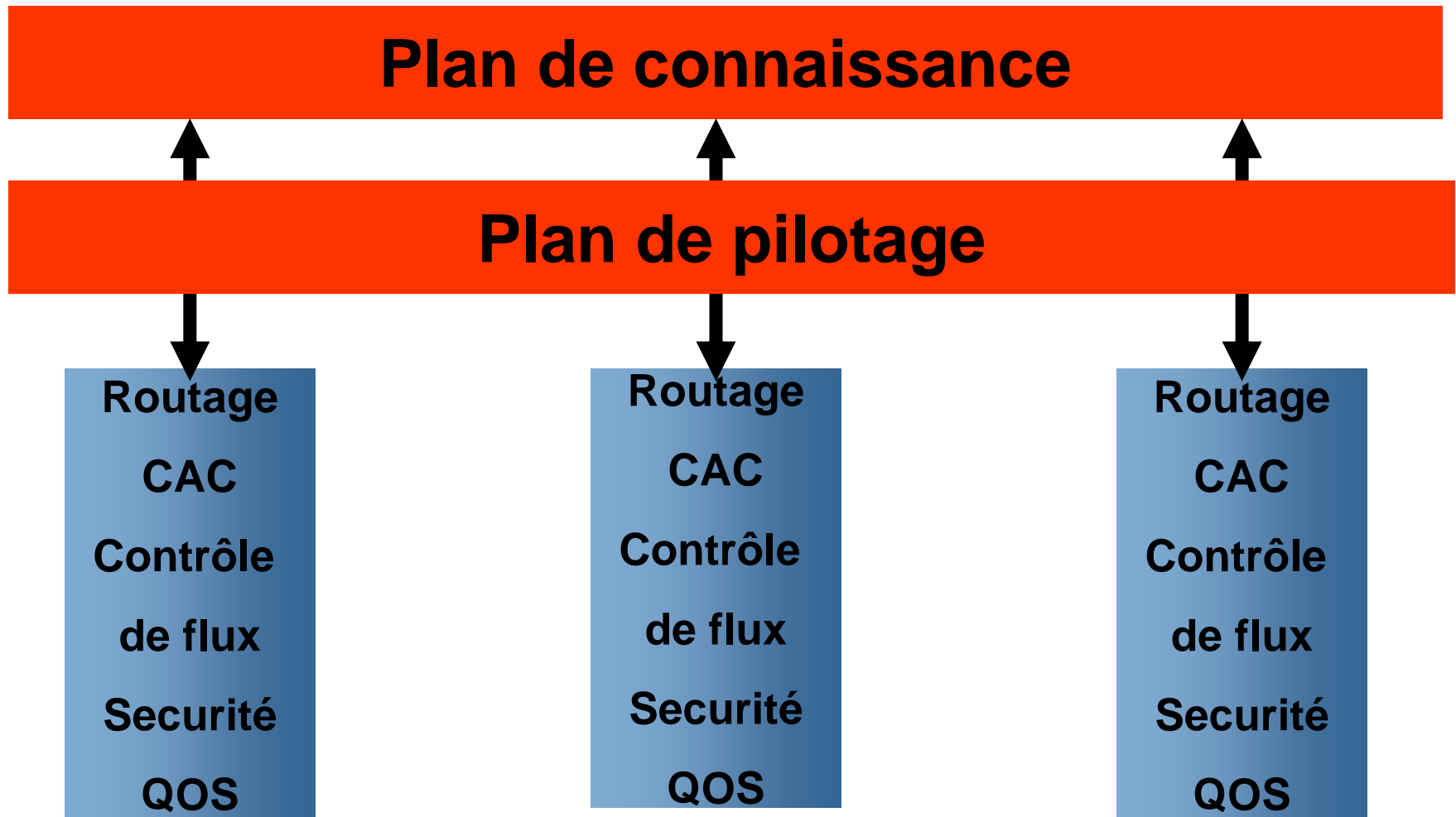
Réseau « autonomic »



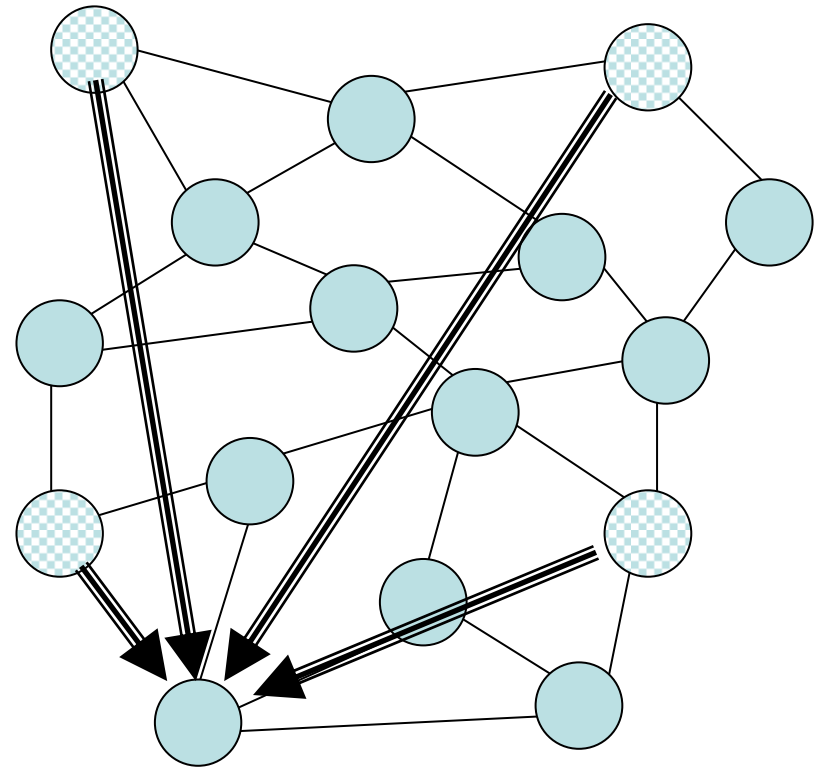
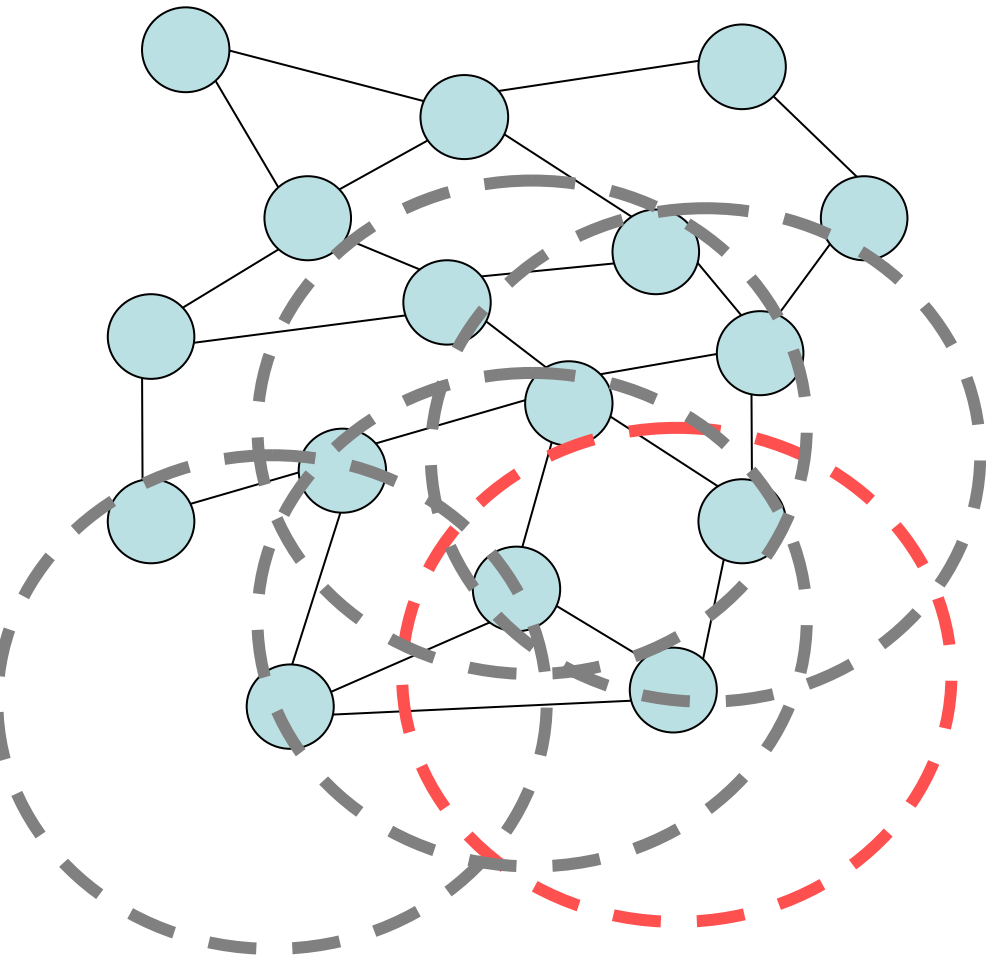
Sans plan de connaissance

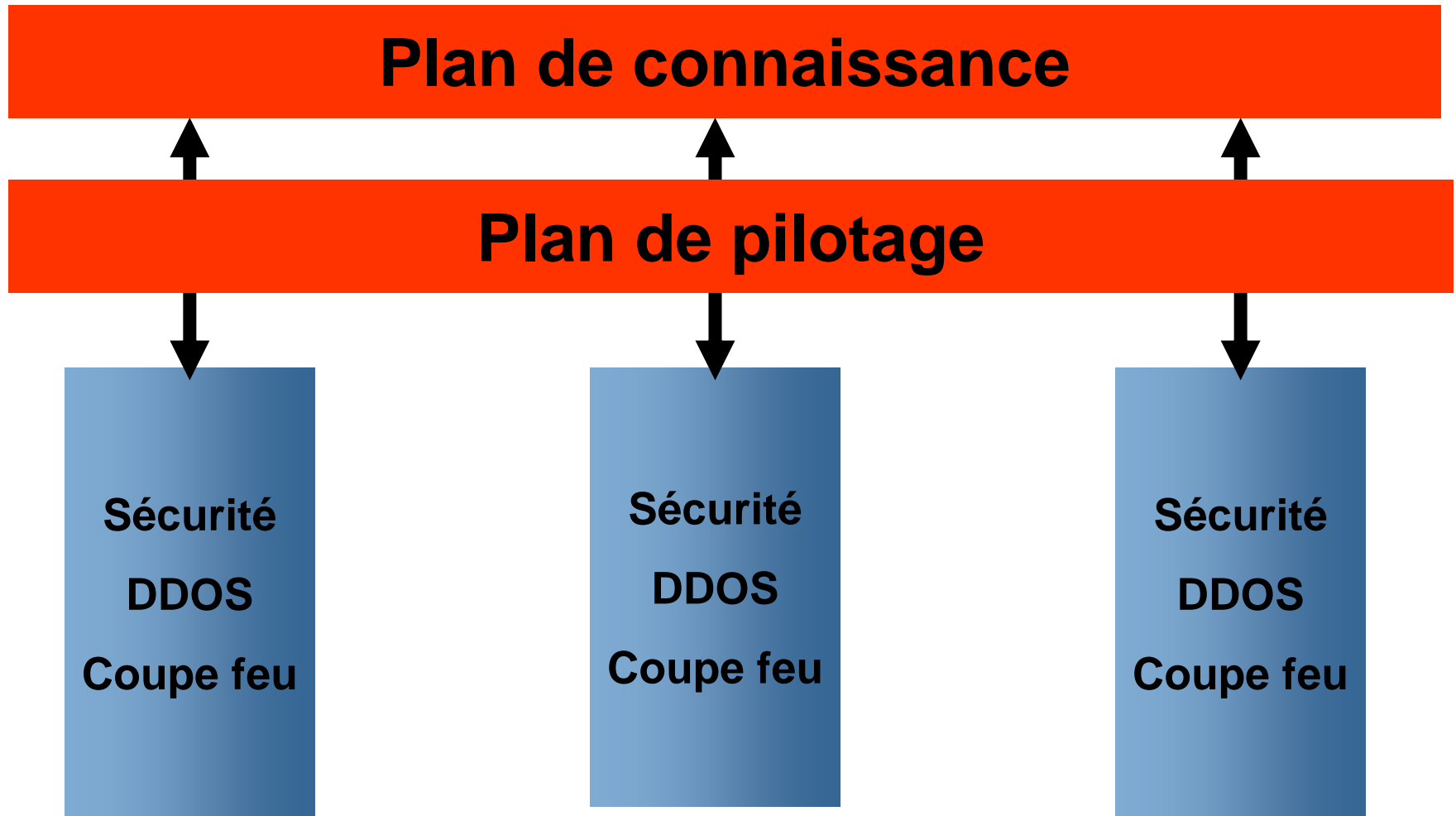


Avec plan de connaissance

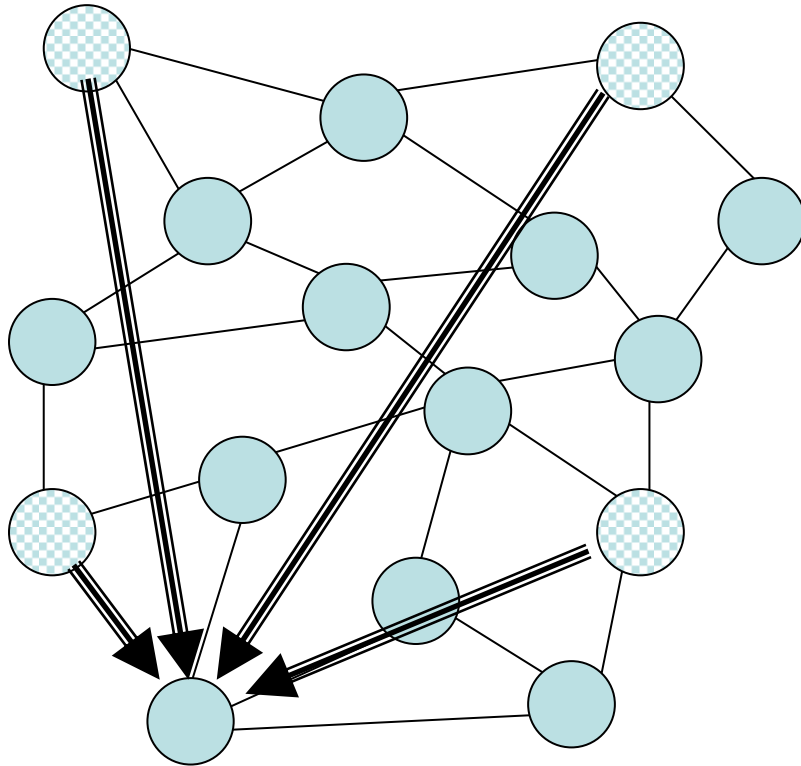


Vue située





Exemple: DDOS



- **La vue située est formée de l'ensemble des routeurs d'accès/ contrôleur**
- **Corrélation des adresses de destination qui apparaissent plus de n fois**
- **Arrêt de l'attaque par destruction des messages DOS**

La virtualisation

Pourquoi la virtualisation?

- **Meilleur amortissement des dépenses d'équipements en utilisant plusieurs réseaux sur une même infrastructure**
- **Partage des ressources**
- **Sécurité des routeurs contre les attaques**
- **Isolation du trafic réseau dans les machines virtuelles**

Virtualisation

• Virtualisation des machines

- Classique

• Virtualisation des OS réseaux

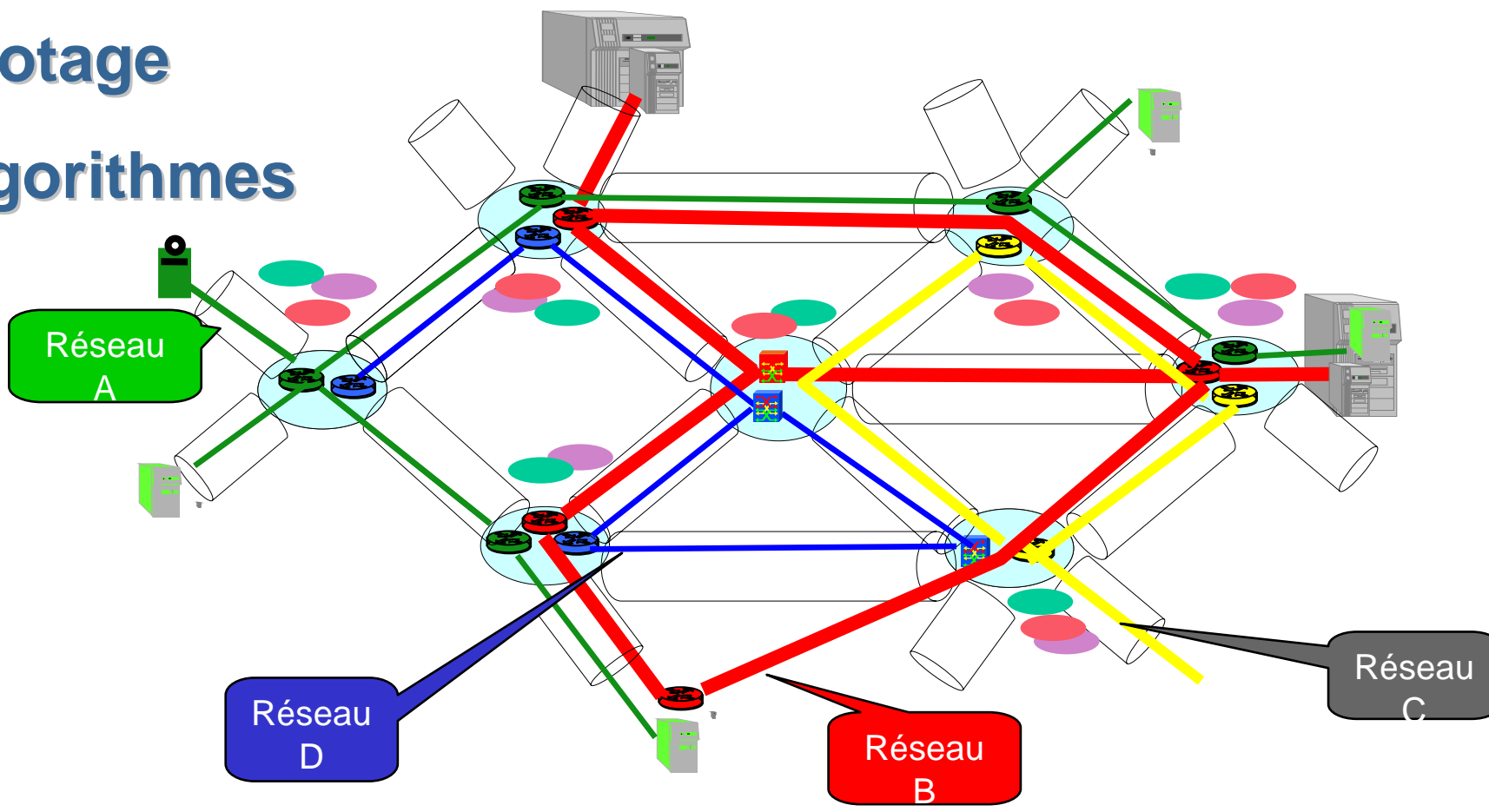
- Virtualisation des plans et des protocoles
 - Plan de connaissance: agent de connaissance virtuel
 - Plan de pilotage: agent de pilotage virtuel
 - Plan de contrôle: algorithme virtuel
 - Plan de données: protocoles virtuels

• Virtualisation des services

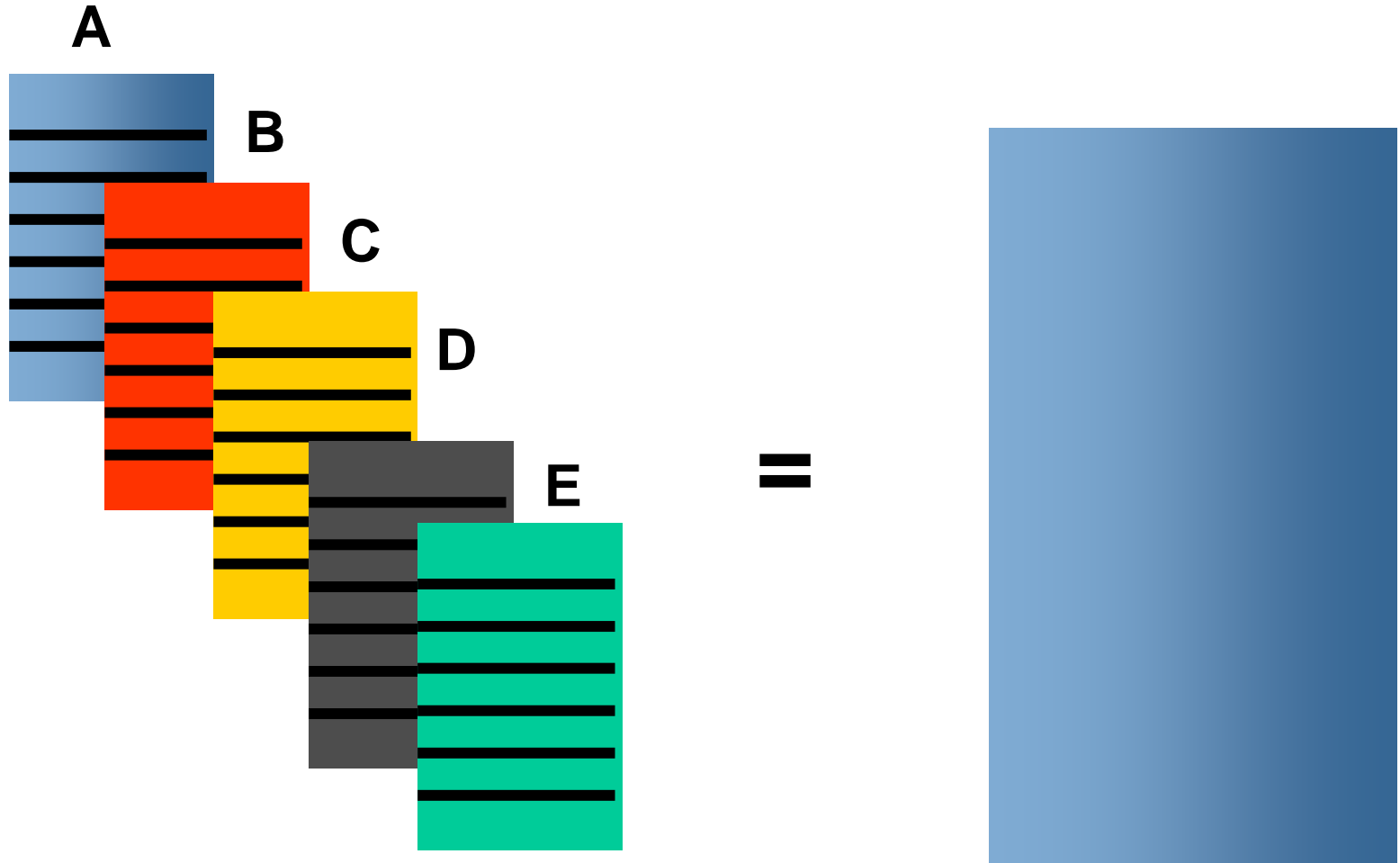
- Classique (data center, centrex, etc.)

Virtualisation

- Agent de connaissance
- Pilotage
- Algorithmes

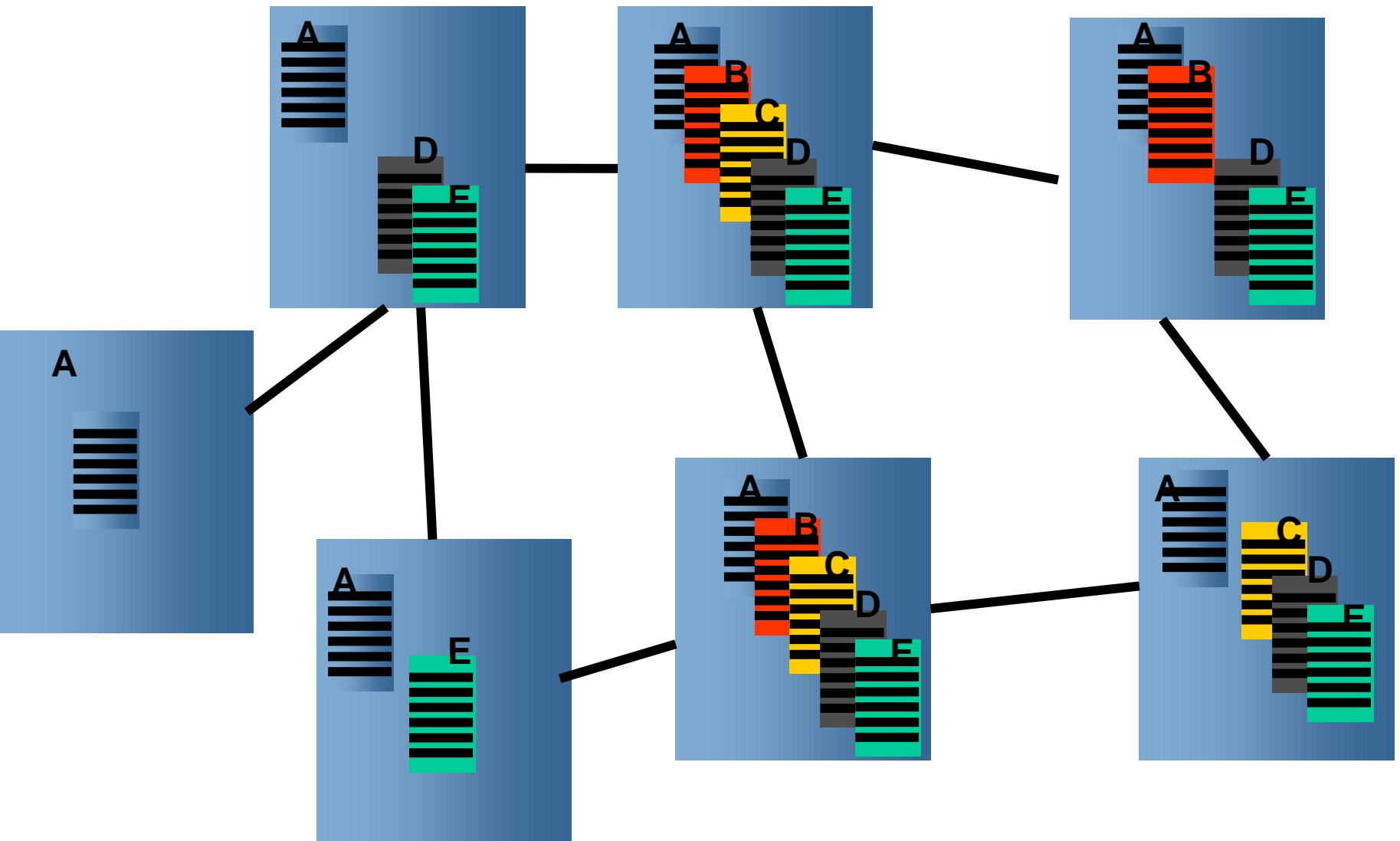


Virtualisation des protocoles



A = pile IP obligatoire

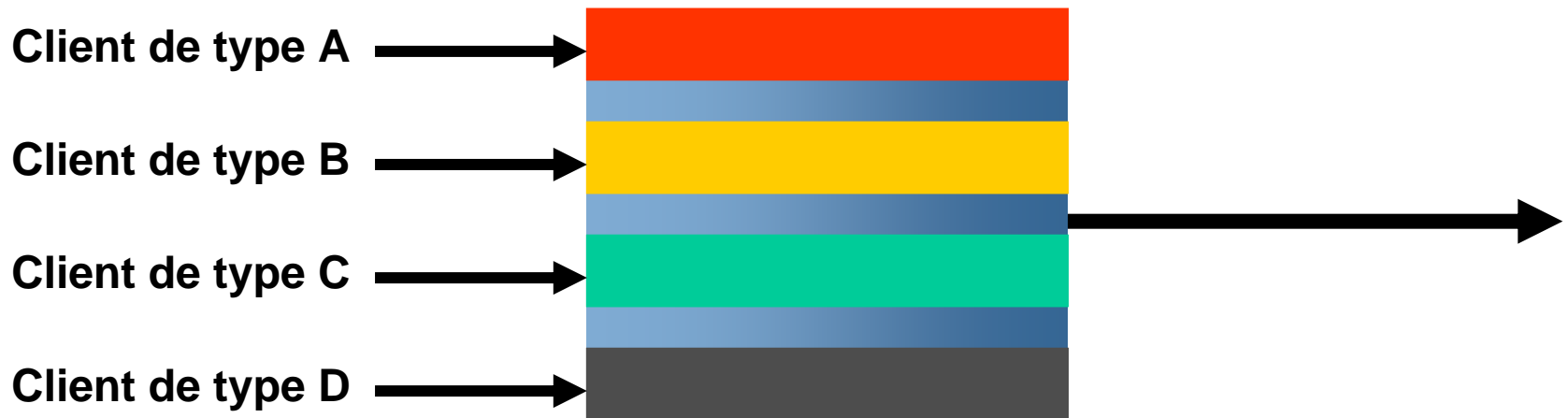
Virtualisation des protocoles



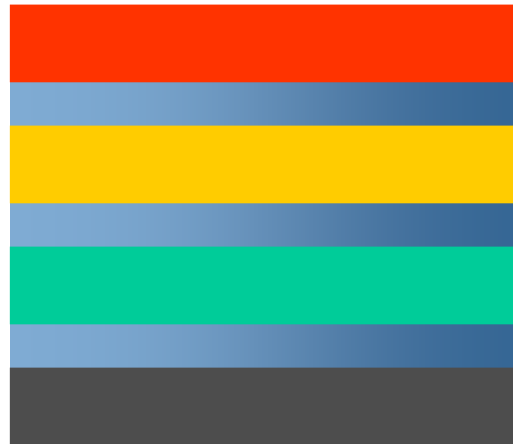
Sécurité des accès

Virtualisation du logiciel dans les points d'accès

- Le point d'accès peut posséder plusieurs OS réseaux avec des SSID différents permettant de traiter la sécurité à différents niveaux

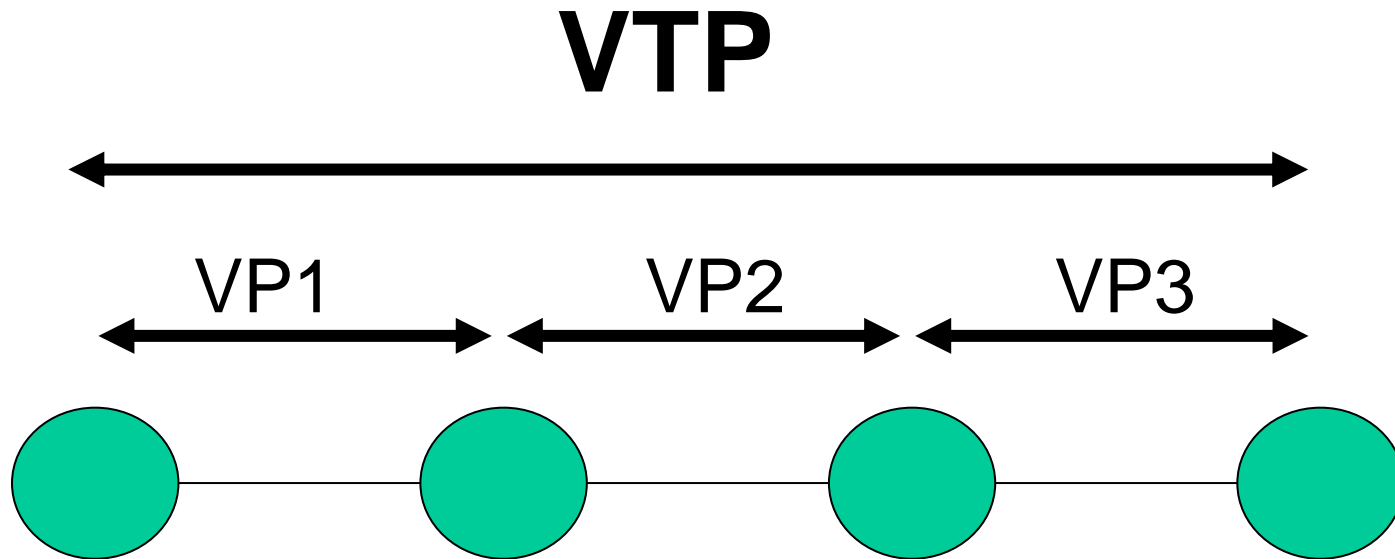


Sécurité du contrôleur



Traitements de sécurité spécifiques dans chaque contrôleur virtuel

VTP/VP (Virtual Transport Protocol/ Virtual Protocol)



Protocole Context-aware

Protocole Virtuel

• VTP/VP (Virtual Transport Protocol/ Virtual Protocol)

• Protocole auto adaptable

■ Capable de s'autopiloter

- Auto adaptation à la sécurité
- Auto adaptation à la QOS
- Auto adaptation à la disponibilité
- Auto adaptation à la mobilité

