

OSSIR

Groupe Windows

Sécurités déployables en WiFi

ONERA, le 13 Juin 2005

Olivier Carbonneaux, Solution Specialist

symbol[®]
The Enterprise Mobility Company™

AGENDA

Qui est Symbol ?

- Le compromis Sécurité/QoS
 - Le besoin historique : la mobilité
- Les particularités d'un système centralisé
- Les architectures de sécurité
 - Le média radio
 - Le VPN adapté radio
 - Les contrôleurs : l'approche DMZ
 - L'intégration du WiFi dans un réseau d'entreprise
- Les solutions de surveillance radio

Qui est Symbol ?

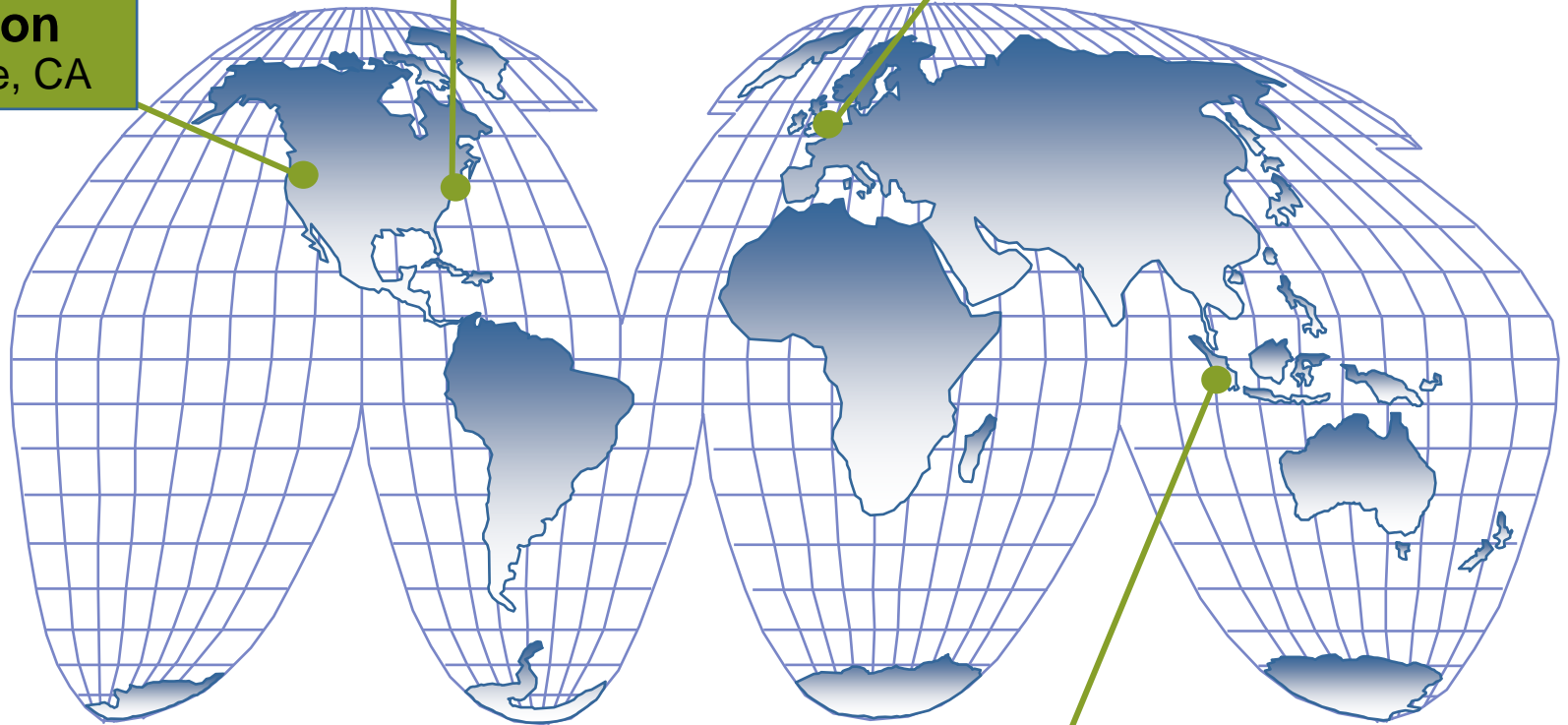
Qui est Symbol ?

symbol[®]
The Enterprise Mobility Company™

**Corporate Headquarters
& TASS Sales Region**
Holtsville, New York

EMEA Sales Region
Berkshire, U.K.

**Wireless
Division**
San Jose, CA



Asia-Pacific Sales Region
Singapore

WorldWide

- Créé en 1975
- Listée au SP500 (NYSE:SBL)
- Market Cap : + 4.0 Mds \$
- 1.7 Mds \$ en 2004
- 5300 personnes

France

- Créé en 1973
- 45M€ en 2004
- 40 personnes



Vision

“Connecter les personnes et les produits aux systèmes d’informations:

Symbol = systèmes de Mobilité”

vision



Saisie de Données
(Claviers, Barcodes, RFID)



capture. move. manage.

MSP

**Réseaux
sans Fil**



Périphériques
(Terminaux endurcis, EDAs)



Un exemple de Mobilité sécurisée

symbol[®]
The Enterprise Mobility Company™



Le compromis Sécurité / QoS

Répondre à des besoins légitimes

- Du point de vue de l'homme réseau :
 - Gérer l'utilisation
 - Installer un backbone radio
 - Sécuriser les transactions
 - Authentifier les utilisateurs avec son annuaire entreprise
- Du point de vue de l'opérationnel :
 - Gérer l'utilisateur
 - Maintenir son application en marche : sortie de couverture, login/mot de passe lourd à supporter
 - Pouvoir évoluer : utiliser le WLAN pour la ToIP avec un EDA, un client fin TSE

Pour répondre aux besoins de mobilité en prenant en compte les préoccupations des équipes réseau, Symbol a proposé bien avant WPA une architecture de sécurité, Kerberos

- Sur la base de WEP
- Conforme à l'implémentation V5 du MIT
- Clé par utilisateur / par session
- Utilisant les facilités d'un serveur Windows 2000
- Puis intégrant le KDC dans l'infrastructure
- Dans le but d'assurer les hand-overs en moins de 50 ms
- Tout en authentifiant mutuellement les éléments du réseau

Un gros souci !

	Kerberos	WPA/EAP	WS5100
802.11 Association	<1ms	<1ms	<1ms
AP-MU Handshake	10ms – 50ms	5ms – 50ms (4-way) 5ms – 20ms (2-way)	5ms – 50ms
AP-Server Handshake	None Required	200ms – 2 seconds	None Required
Total	≤ 50ms	250ms – 3 seconds	≤ 50ms

Un système centralisé

Des attentes différentes...

symbol[®]
The Enterprise Mobility Company™

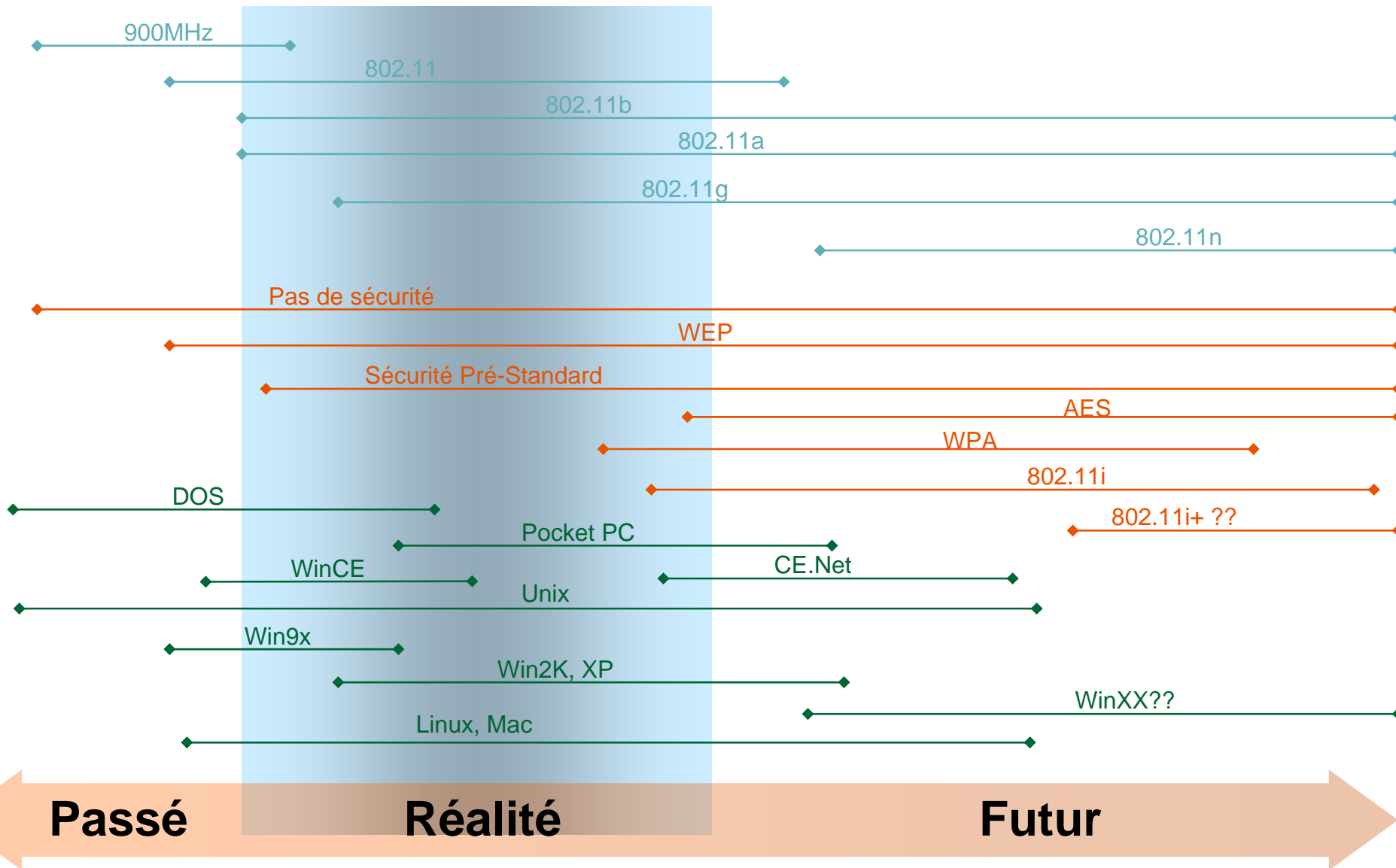
A man in a dark suit, white shirt, and dark tie is shown from the chest up. He has a serious expression and is looking slightly to the right. The background is a solid light blue. Three thought bubbles of varying sizes trail from his head towards the top left. Two callout bubbles, one oval and one speech bubble, point towards him from the right side.

SECURITE

PERIPHERIQUE
CLIENT

INFRASTRUCTURE

Ce qui se passe, dans la réalité



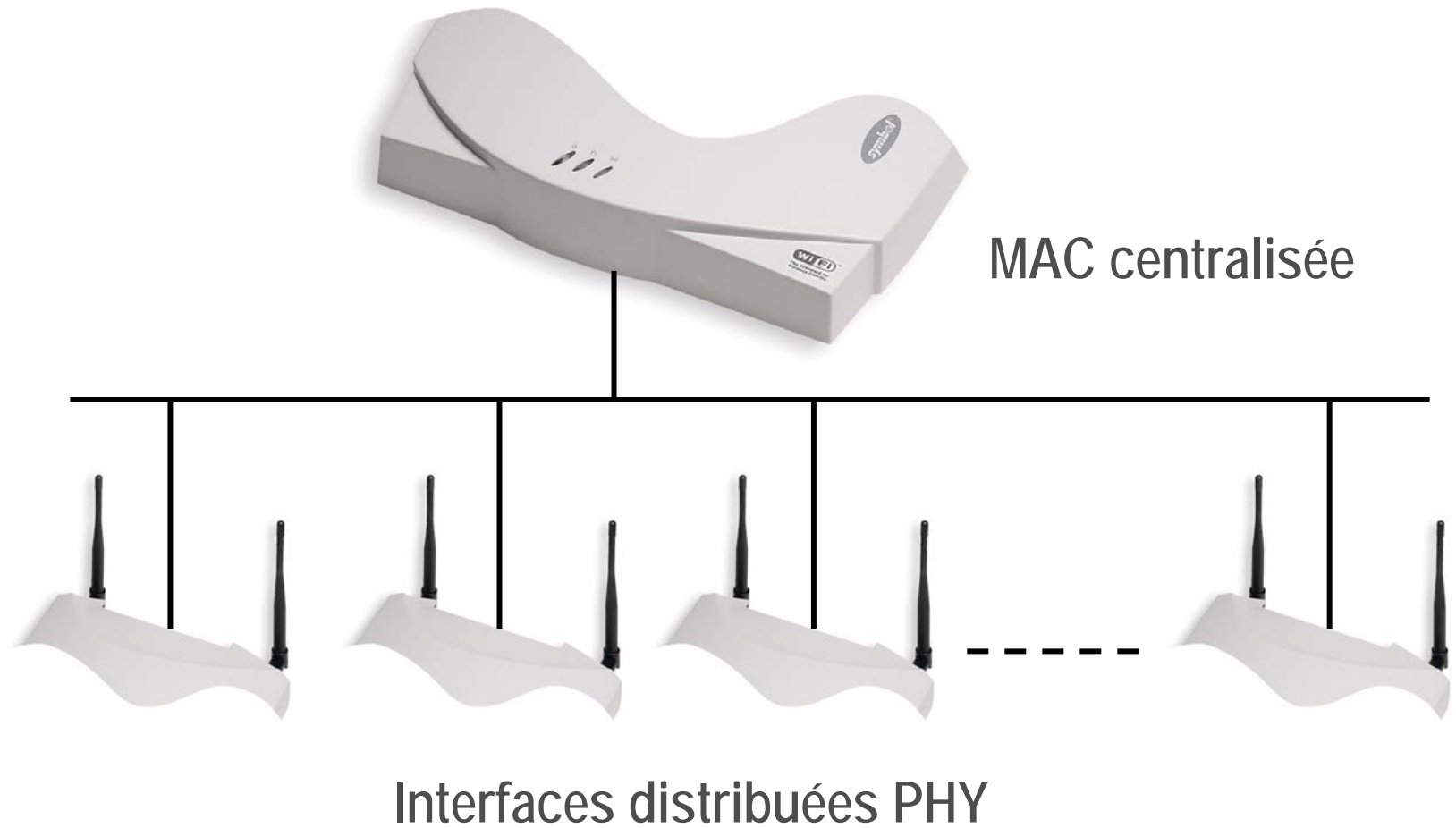
Découpage fonctionnel d'un AP



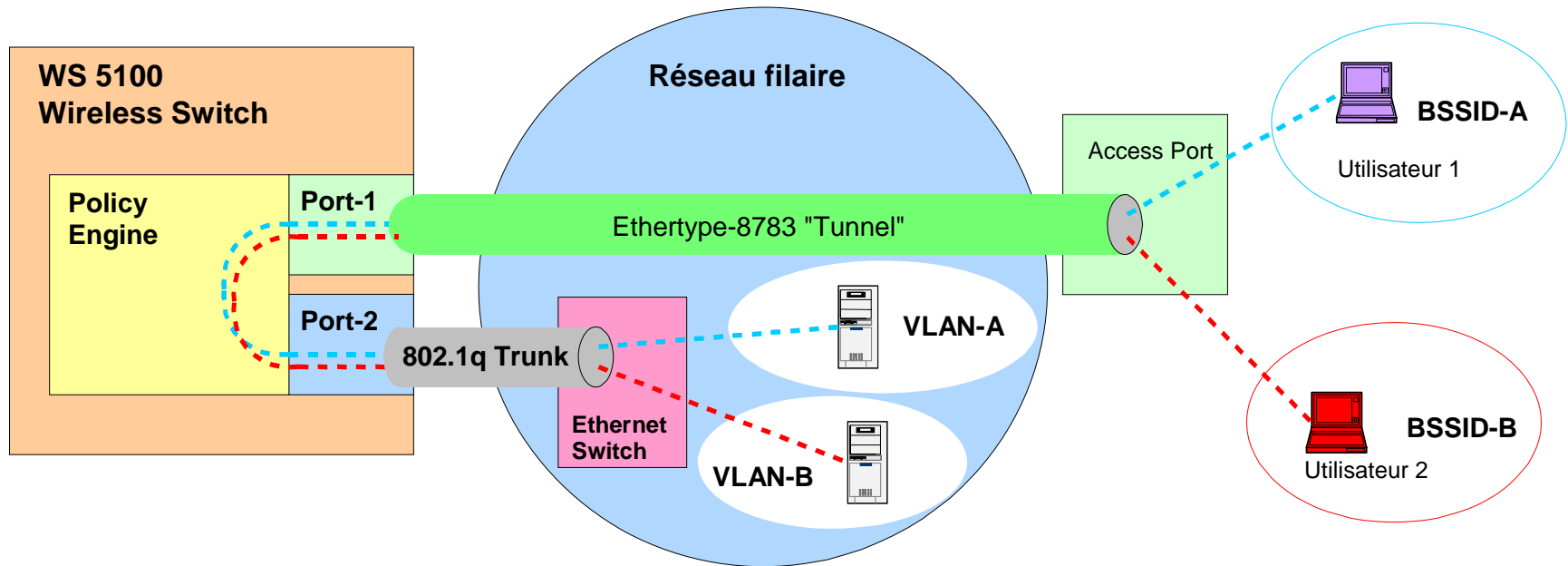
- **PHY**
- Radio
 - ▶ 802.11
 - ▶ 802.11b
 - ▶ 802.11a
 - ▶ 802.11g
 - ▶ 802.11abg
- Coût faible
- **MAC**
- Media Access Control
- CPU & mémoire
- Fonctionnalités
- Coût plus élevé

Et si . . .

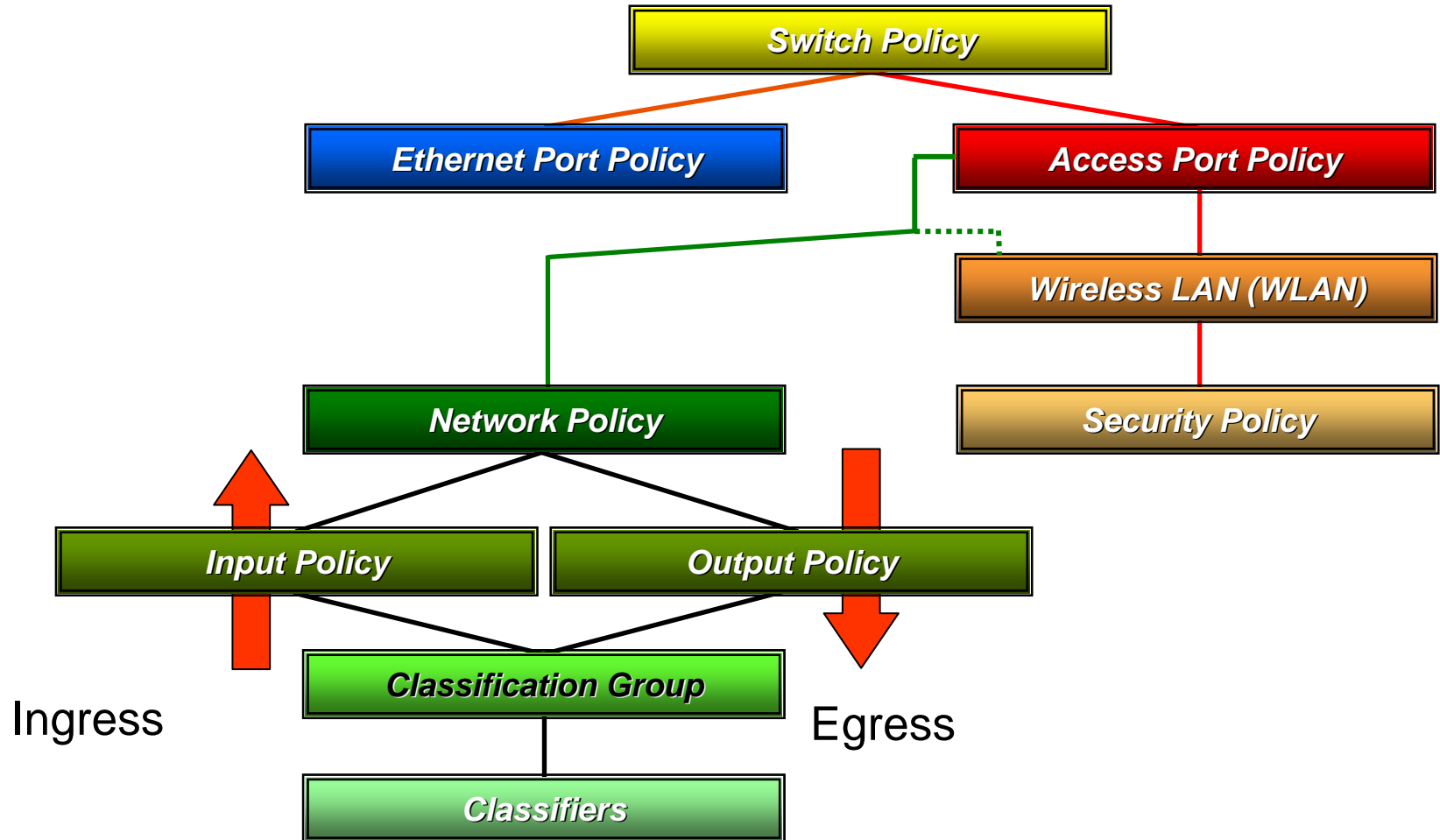
symbol[®]
The Enterprise Mobility Company™



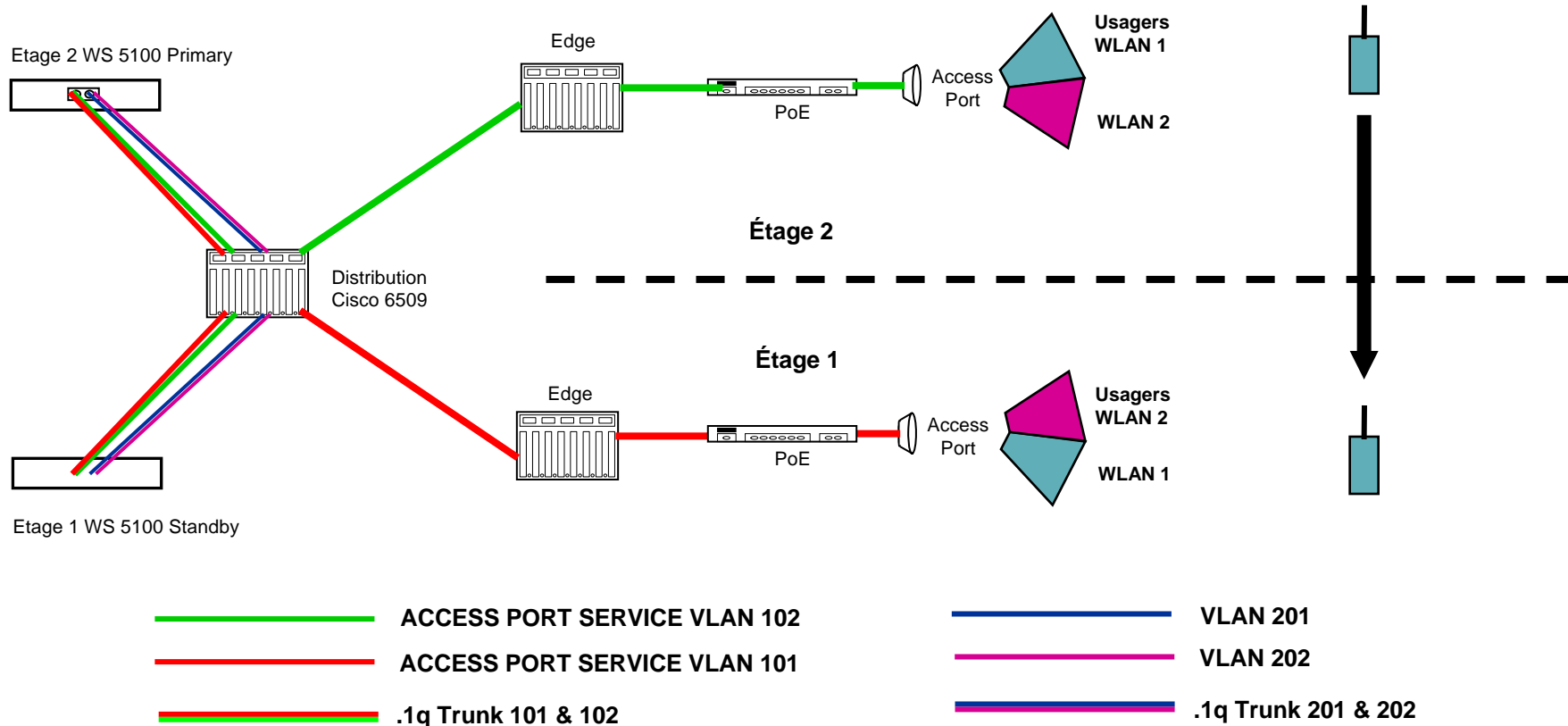
Comment ça marche ?



C'est le prolongement du fil : un VLAN = un BSSID
Le WS est en coupure des flux WiFi



L'intérêt !



Question 1: quel serait l'architecture en AP lourd ?
Question 2: en AP lourd, où va le VLAN de management ?

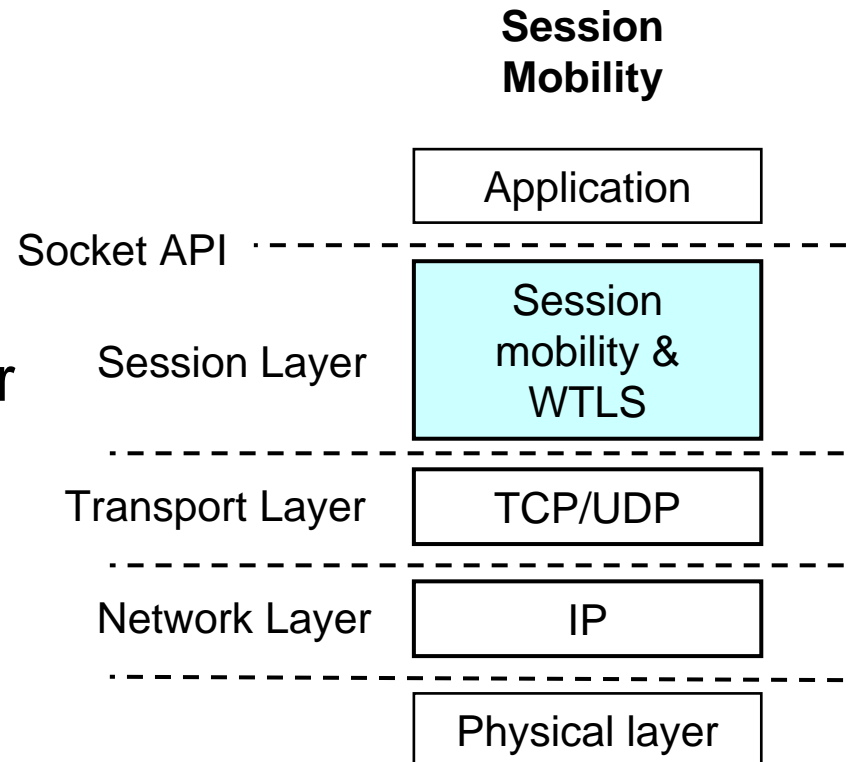
Les architectures de sécurité

Le WiFi n'est pas magique, désolé ☹ !

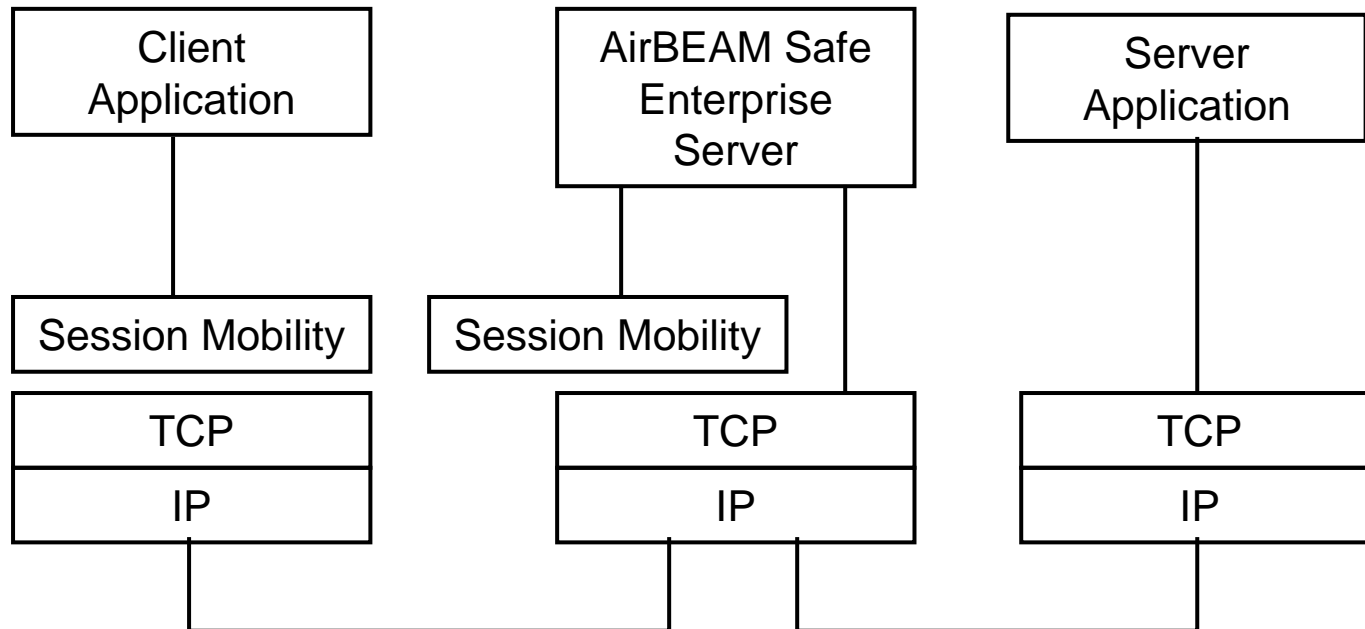
- Sensible à tout déni de service
 - Trames de management non sécurisées
- Utilise une bande partagée, la 2.4Ghz
 - Bande Industrial Scientific Medical
 - Transmetteurs vidéo
 - Radars d'intrusion
 - Domotique
- La bande 5GHz est plus propre
 - Pas de souci de compatibilité
- Ne pas confondre sécurité du réseau et disponibilité

L'intérêt

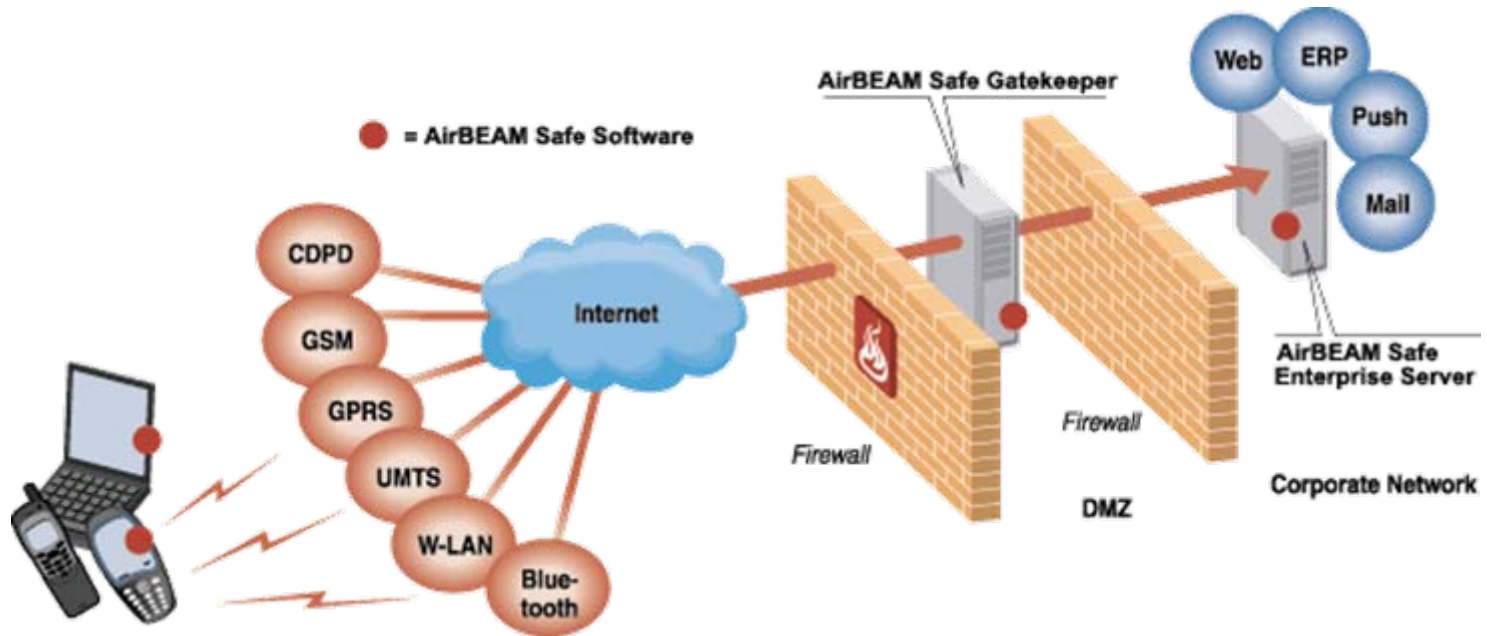
- Renégocie sa connexion à chaque média
- Comprime avant de chiffrer
 - Pas IPSec
- Évalue le meilleur média en permanence



Une solution VPN adaptée



AirBeam Safe



Avantages

- Indépendant des réseaux WiFi, des clients
- Point de passage unique des flux WiFi **et** filaire
- Permet de sécuriser des OS non WPA/WPA2
- Fournit des contrôles supplémentaires (BP)
- Souple (utilisateurs temporaires)

Inconvénients

- Une gestion supplémentaire : équipe réseaux ?
- Onéreux
- Point de passage unique = point de faiblesse ?

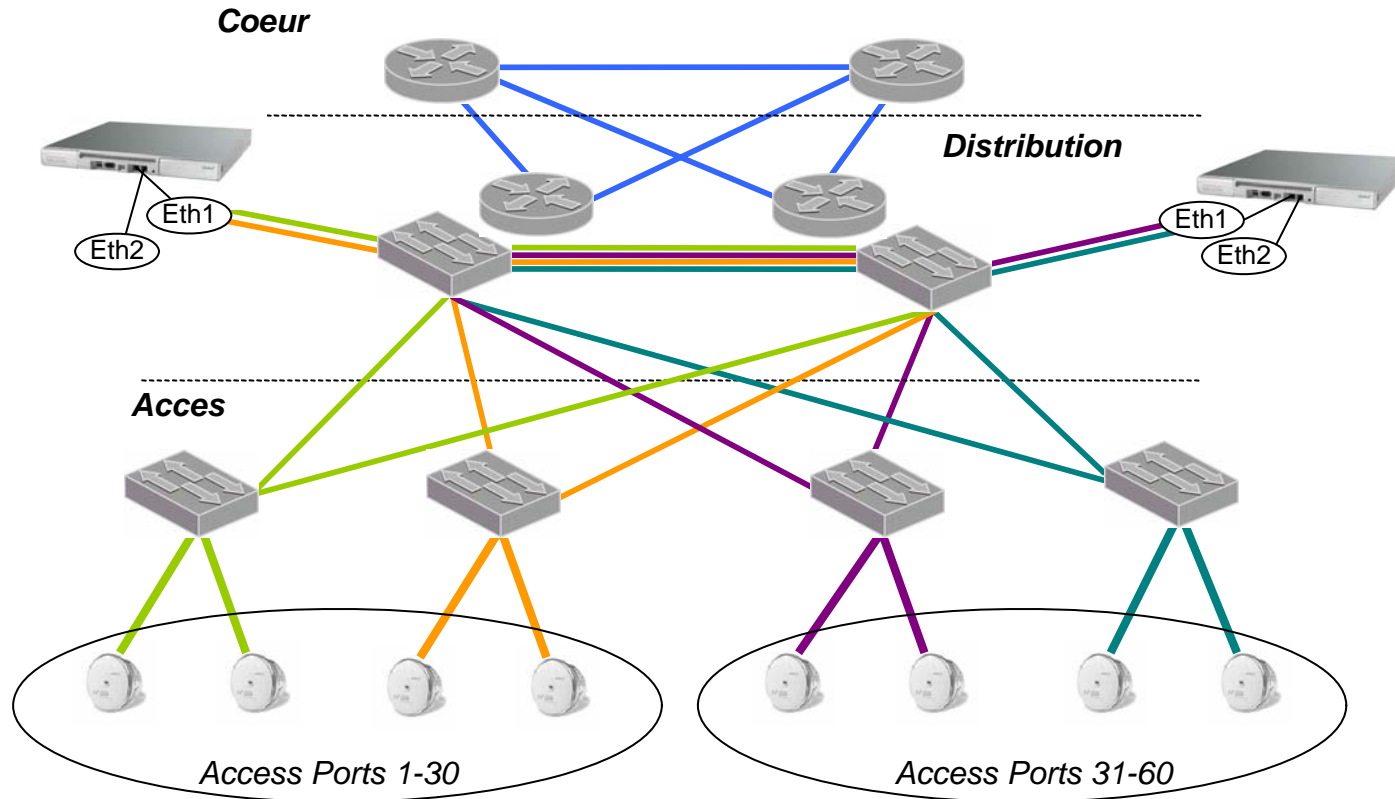
Utilisation de WPA Entreprise à minimum, mais à maximum aussi !

- WindowsXP-KB826942-x86-FRA.exe...
- Manque de matériels/firmwares/drivers sous WPA2 (WindowsXP-KB893357-v2-x86-FRA.exe)
- Les équipes informatiques n'ont pas toutes validées le SP2 de XP, qui ne suffit pas...
- Mobile 2003 ne le supporte pas
- Les constructeurs entreprise quittent le marché de la carte
 - Modules embarqués

Radius est incontournable, de plus en plus embarqué, et les connecteurs LDAP arrivent, exemple du WS2000

The screenshot displays the configuration interface for a WS 2000 Wireless Switch. The left sidebar shows a tree view of configuration categories, with 'LDAP' selected under 'Radius Server'. The main panel, titled 'LDAP', contains the following configuration fields:

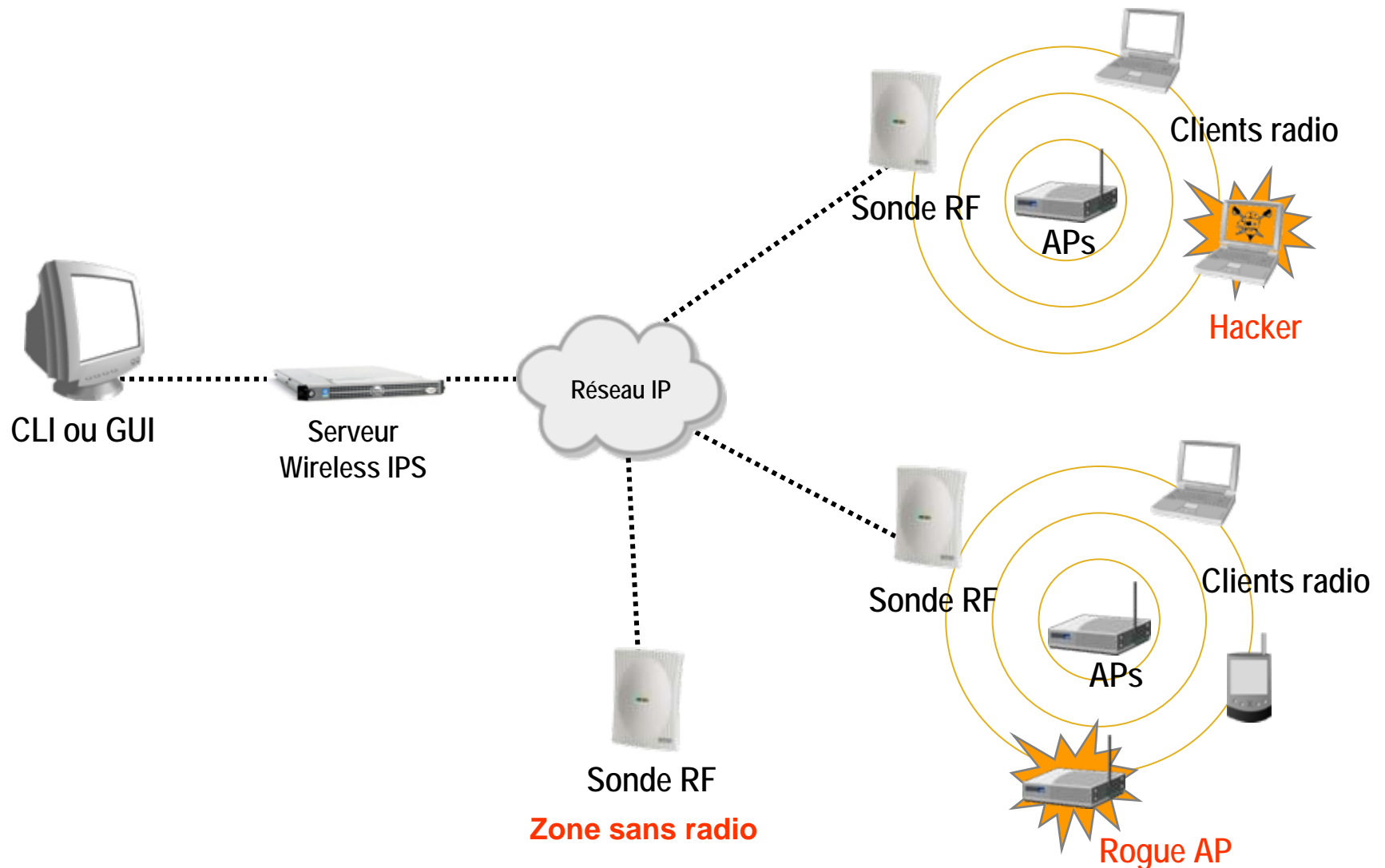
Field	Value
LDAP Server IP	157 . 235 . 91 . 2
Port	389
Login Attribute	(uid=%{Stripped-Us
Password Attribute	userPassword
Bind Distinguished Name	cn=Manager,o=mob
Password	
Base Distinguished Name	o=mobion
Group Attribute	cn
Group Filter	(&(&(objectClass=GroupOfNames)(mem
Group Membership Attribute	radiusGroupName

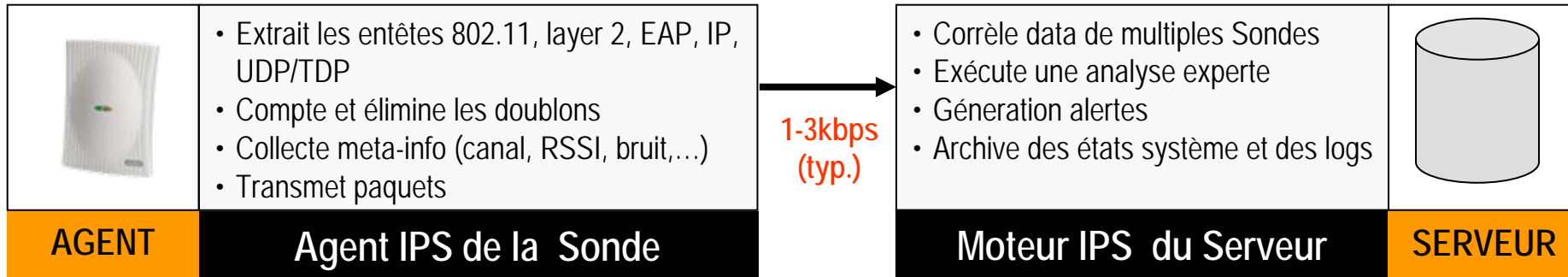


- De manière générale, Symbol préconise une approche « VLAN in a box » : le réseau est segmenté, prévisible, déterministe, car géré par le fil

La surveillance radio

Topologie Wireless IPS





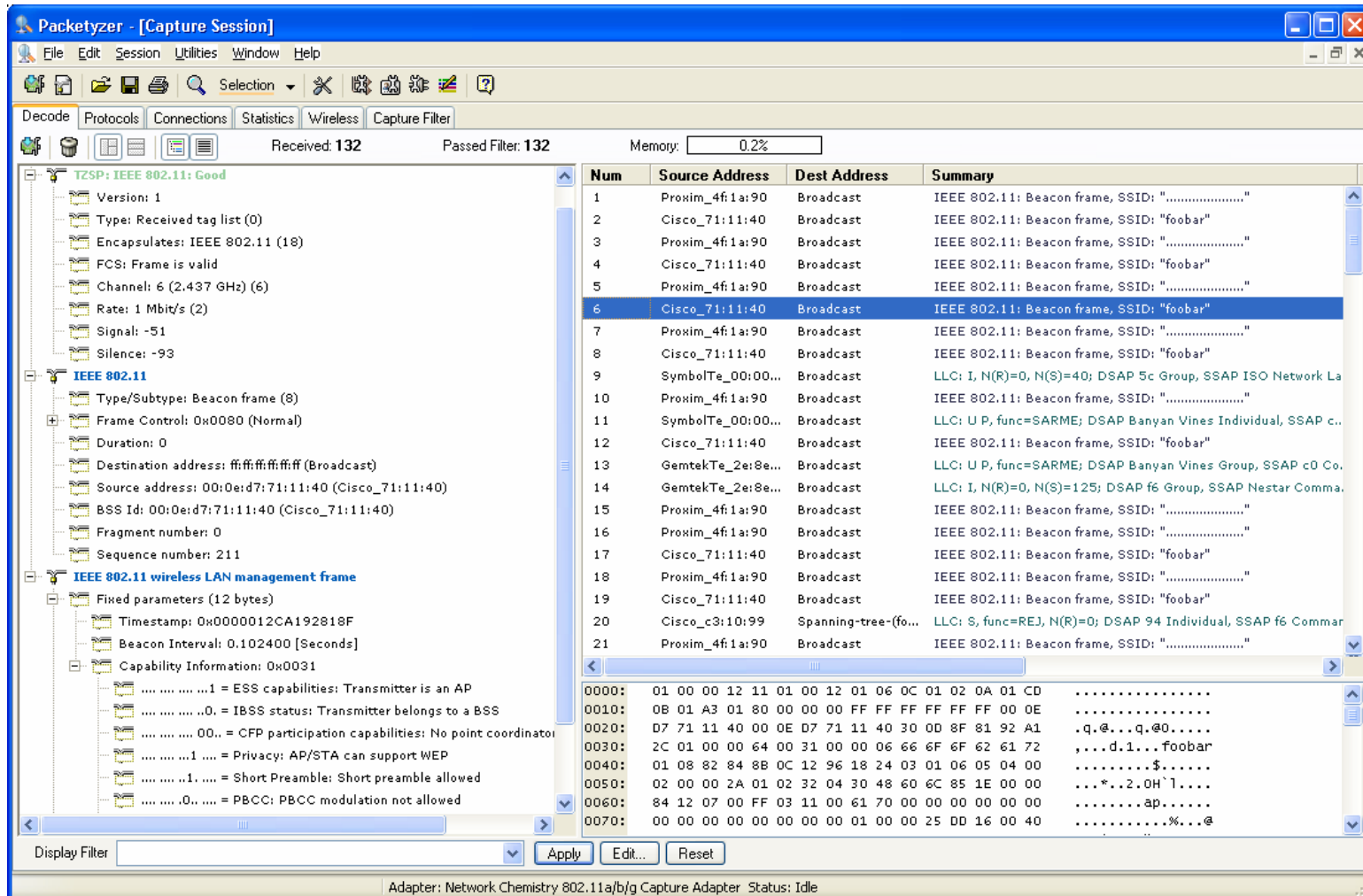
Partage la charge de l'analyse entre la sonde et le serveur

- Minimise la charge réseau
- Minimise les upgrades sur les sondes
- Maximalise la précision de l'analyse grâce à la corrélation du serveur

Nouveaux algorithmes de détection = Upgrade serveur

- Pas besoin de mettre à jour les sondes tous les mois
- Pas besoin de re-qualifier de nouveaux firmwares

Capture de trafic



Packetyzer - [Capture Session]

File Edit Session Utilities Window Help

Decode Protocols Connections Statistics Wireless Capture Filter

Received: 132 Passed Filter: 132 Memory: 0.2%

TZSP: IEEE 802.11: Good

- Version: 1
- Type: Received tag list (0)
- Encapsulates: IEEE 802.11 (18)
- FCS: Frame is valid
- Channel: 6 (2.437 GHz) (6)
- Rate: 1 Mbit/s (2)
- Signal: -51
- Silence: -93

IEEE 802.11

- Type/Subtype: Beacon frame (8)
- Frame Control: 0x0080 (Normal)
- Duration: 0
- Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
- Source address: 00:0e:d7:71:11:40 (Cisco_71:11:40)
- BSS Id: 00:0e:d7:71:11:40 (Cisco_71:11:40)
- Fragment number: 0
- Sequence number: 211

IEEE 802.11 wireless LAN management frame

- Fixed parameters (12 bytes)
- Timestamp: 0x0000012CA192818F
- Beacon Interval: 0.102400 [Seconds]
- Capability Information: 0x0031
 -1 = ESS capabilities: Transmitter is an AP
 -0, = IBSS status: Transmitter belongs to a BSS
 -00.. = CFP participation capabilities: No point coordinator
 -1 = Privacy: AP/STA can support WEP
 -1. = Short Preamble: Short preamble allowed
 -0. = PBCC: PBCC modulation not allowed

Num	Source Address	Dest Address	Summary
1	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
2	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
3	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
4	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
5	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
6	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
7	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
8	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
9	SymbolTe_00:00:00...	Broadcast	LLC: I, N(R)=0, N(S)=40; DSAP 5c Group, SSAP ISO Network La
10	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
11	SymbolTe_00:00:00...	Broadcast	LLC: U P, func=SARME; DSAP Banyan Vines Individual, SSAP c..
12	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
13	GemtekTe_2e:8e:8e...	Broadcast	LLC: U P, func=SARME; DSAP Banyan Vines Group, SSAP c0 Co.
14	GemtekTe_2e:8e:8e...	Broadcast	LLC: I, N(R)=0, N(S)=125; DSAP f6 Group, SSAP Nestar Comma.
15	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
16	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
17	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
18	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."
19	Cisco_71:11:40	Broadcast	IEEE 802.11: Beacon frame, SSID: "foobar"
20	Cisco_c3:10:99	Spanning-tree-(fo...	LLC: S, func=REJ, N(R)=0; DSAP 94 Individual, SSAP f6 Commar
21	Proxim_4f:1a:90	Broadcast	IEEE 802.11: Beacon frame, SSID: "....."

0000: 01 00 00 12 11 01 00 12 01 06 0C 01 02 0A 01 CD
0010: 0B 01 A3 01 80 00 00 00 FF FF FF FF FF FF 00 0E
0020: D7 71 11 40 00 0E D7 71 11 40 30 0D 8F 81 92 A1 .q.@...q.@0....
0030: 2C 01 00 00 64 00 31 00 00 06 66 6F 6F 62 61 72 ...d.1...foobar
0040: 01 08 82 84 8B 0C 12 96 18 24 03 01 06 05 04 00\$.
0050: 02 00 00 2A 01 02 32 04 30 48 60 6C 85 1E 00 00 ...*.2.0H'1....
0060: 84 12 07 00 FF 03 11 00 61 70 00 00 00 00 00 00ap.....
0070: 00 00 00 00 00 00 00 00 01 00 00 25 DD 16 00 40%...@

Display Filter [] Apply Edit... Reset

Adapter: Network.Chemistry 802.11a/b/g Capture Adapter Status: Idle

Ce qui est détecté...



Vulnerability

1. AP Broadcasting SSID
2. AP is Not Allowed Vendor Type
3. AP is Not Using Encryption
4. AP is Using Default SSID
5. AP is Using Hotspot SSID
6. Ad-Hoc Network Operating
7. Client (Authorized) Connected to Rogue AP
8. Client (Rogue) Connected to Authorized AP
9. Client is Not Allowed Vendor Type
10. Client Roaming Outside Allowed Areas
11. NetBIOS Traffic
12. Rogue AP Detected
13. Rogue Ad-Hoc Client Detected
14. Rogue Client Detected
15. Rogue softAP Detected
16. Service Van Nearby
17. Station is Operating as Unauthorized Type
18. Station Not Using 802.1x
19. Station Not Using Fortress Encryption
20. Station Not Using PEAP
21. Station Not Using TKIP
22. Station Not Using VPN
23. Station Not Using WPA in PSK Mode
24. Station Using Open Authentication
25. Station Using Weak WEP IVs
26. Wireless Use Outside of Allowed Hours

Reconnaissance

1. APHopper Detected
2. Client (Authorized) Probing for Any Access Point
3. Client (Rogue) Probing for Any Access Point
4. NetStumbler Detected
5. Wellenreiter Detected

Denial of Service

1. AP Overload
2. Association Storm
3. Authentication Storm
4. Broadcast Deauthentication Packet
5. Broadcast Dissociation Packet
6. Deauthentication Storm
7. Dissociation Storm
8. Duration Attack Detected
9. EAPoL Logoff Storm
10. EAPoL Start Storm
11. Fata-Jack Attack Detected
12. Improper Broadcast Packet
13. MIC Failure Based DoS Detected
14. Omerta Attack Detected
15. RF Jamming Detected



Ce qui est détecté...voire neutralisé !



Intrusion

1. AP Channel Change
2. AP SSID Change
3. Adhoc SSID Same as Authorized AP
4. Airjack Attack Detected
5. Airpwn Attack Detected
6. Airsnarf Attack Detected
7. ASLEAP Attack Detected
8. Authorized AP Dened Association
9. Authorized AP Denied Authentication
10. Constant Traffic Sent/Received by Authorized Client
11. Constant Traffic Sent/Received by Rogue Client
12. Fake AP Operating
13. Fake Client Operating
14. Hotspotter Attack Detected
15. Possible Worm Traffic
16. RADIUS Dictionary Attack Detected
17. Rogue AP Using SSID of Authorized AP
18. Spoofed MAC Address
19. Spurious Traffic Sent by Client
20. Station is Using Random MAC Address
21. WEPWedgie Attack Detected

Operational

1. AP Failure or Missing [CustomProtect]
2. AP Low Signal Strength
3. AP Reported a Problem to a Client
4. AP Supports Multiple SSIDs
5. AP Restarted
6. Association Failure or Problem
7. Authentication Failure or Problem
8. Authentication (802.1x) Failure or Problem
9. Channel With Too Many APs
10. Channel With Excessive Errors
11. Client BSSID Changed
12. Client Failure or Missing [CustomProtect]
13. Client is Roaming [CustomProtect]
14. Client is Roaming Too Quickly
15. Client Rate Support Mismatch
16. New AP Discovered
17. New softAP Discovered
18. New Ad-Hoc Client Discovered
19. New Client Discovered
20. Excessive Low Speed Traffic
21. Station with Excess Retransmissions
22. Turbocell in Use
23. Wireless Bridge Detected (WDS Mode)
24. Wireless Bridge Detected (Non-WDS Mode)

System

1. RFprotect Engine Started
2. RFprotect Engine Stopped
3. Client Actively Prevented From Using AP
4. Initiating Active Containment of AP
5. Initiating Active Containment of Client
6. Sensor Configuration Changed
7. Sensor Failed to Start
8. Sensor Missed Keep-Alive
9. Sensor Operating in Packet Capture Mode