Architecture de réseau WiFi centralisée Cisco

Une approche simplifiée de la gestion des réseaux sans-fil

UMLV / Ingénieurs 2000
Xposé - IR3 - 2009/2010

Jean-Christophe Rios

Sommaire

1. De quoi parle-t-on ?
2. Architecture autonome
3. Architecture centralisée
4. Protocole d'échange: LWAPP
5. Bibliographie

Sommaire

1. De quoi parle-t-on ?

- WiFi: bref historique:
  - 1999: 802.11b
    - Les débuts
    - Peu utilisé en entreprise (peu de matériel)
  - Période 2002-2005: généralisation des accès sans-fil
    - Proposer une connexion sans-fil en environnement entreprise
    - A l'époque, une simple connectivité
  - Plus récemment: volonté de proposer plus

1. De quoi parle-t-on ?

- Infrastructure de réseau sans-fil IEEE 802.11x
- Un réseau WiFi est constitué d'un ensemble de points d'accès (AP)
  - On s'intéresse à la gestion des composants du réseau (point de vue administrateur)
- Comment organise-t-on un tel réseau ?
  - Quelles sont les architectures disponibles ?

Sommaire

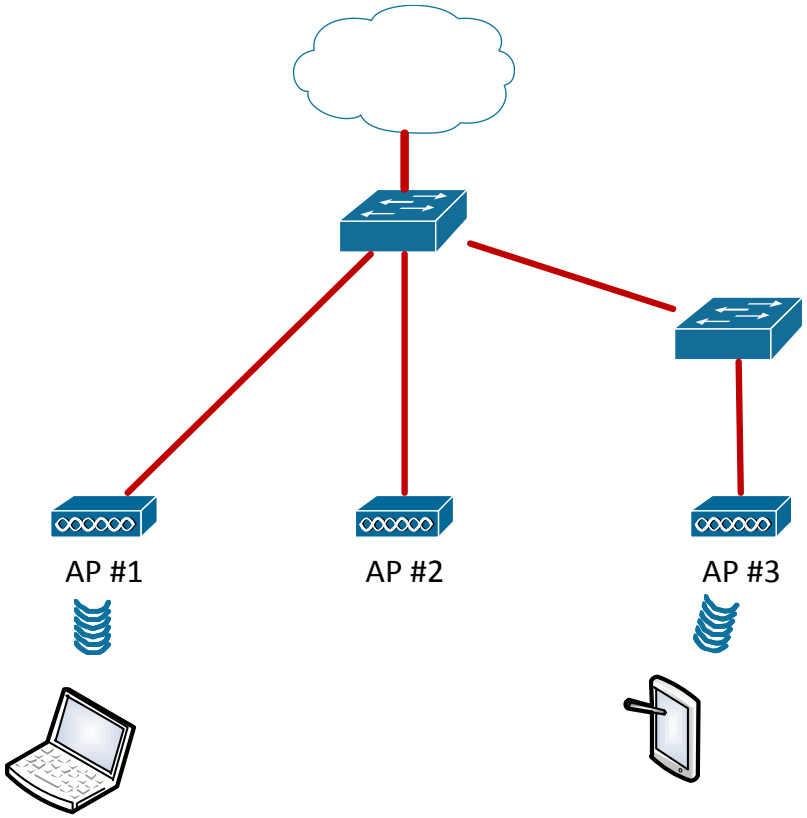
1. De quoi parle-t-on ?
2. Architecture autonome
3. Architecture centralisée
4. Protocole d'échange: LWAPP
5. Bibliographie

2. Architecture « autonome »

- Solution « classique », largement déployée

- Réseau constitué d'un ensemble d'AP autonomes
  - Agissent comme des éléments indépendants
  - Chaque AP:
    - Est un élément autonome du réseau
    - A sa propre version de configuration
    - Prend en charge un certain nombre de tâches par lui-même

Schéma d’architecture autonome



AP autonome: caractéristiques

- Elément autonome du réseau:
  - Assimilable à un commutateur
  - Gestion RF (radiofréquences)
  - Gestion des associations 802.11
  - Gestion de la sécurité :
    - Clés de chiffrement (si utilisation de PSK)
    - Autorisations d'accès (*authenticator* 802.1x)

Limites

- Gestion individuelle des AP, fastidieuse
  - Une version de configuration par AP
    - Changement => modifier tous les AP
- Pas de coordination des politiques RF
  - À définir manuellement, c'est parfois difficile
- Lourdeur d'implantation
  - Diffusion et propagation de tous les VLAN client au port de connexion
- Pas de gestion intelligente de la mobilité (*handover/roaming*)
- Pas de vue globale du réseau
  - À moins d'implémenter sa propre solution de *monitoring* et *reporting*

Sommaire

1. De quoi parle-t-on ?
2. Architecture autonome
3. Architecture centralisée
4. Protocole d'échange: LWAPP
5. Bibliographie

3. Architecture centralisée

- Concepts fondamentaux:
  - Concentrer l'intelligence en un point unique
  - Les AP doivent être de simples antennes
- Eléments constitutifs:
  - Points d'accès légers (LAP, *Lightweight Access Point*)
  - Contrôleurs
  - Serveur(s) d'administration
- On présente ici la solution Cisco « CUW » (*Cisco Unified Wireless*)
  - Des solutions concurrentes existent:
    - Aruba Networks
    - Bluesocket

Schéma d’architecture centralisée

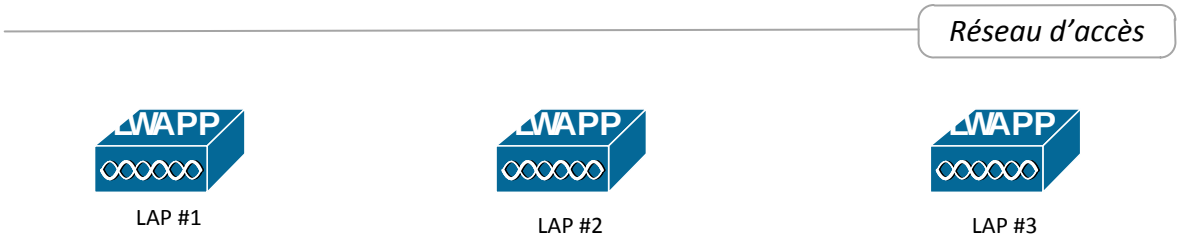


Schéma d'architecture centralisée

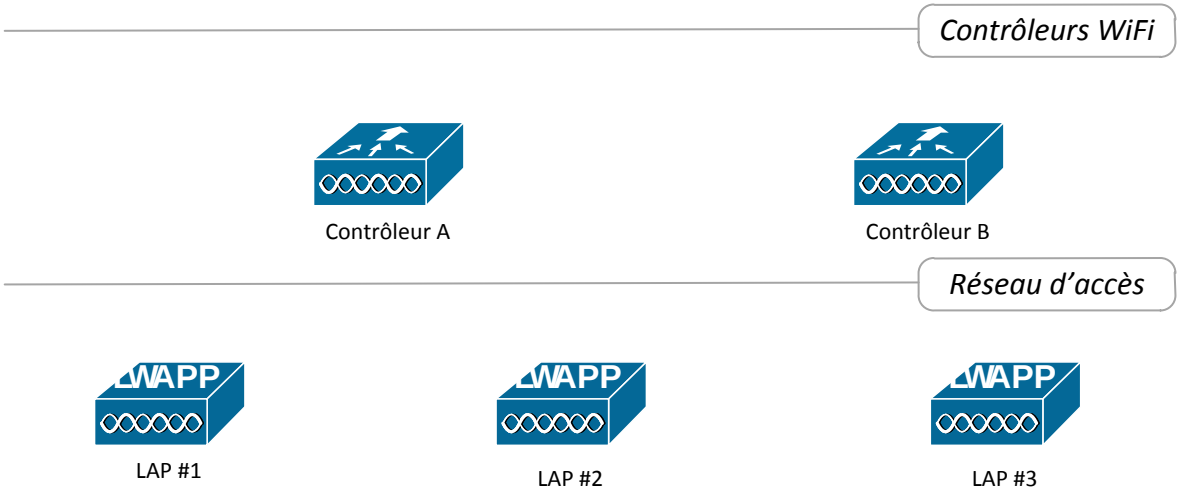


Schéma d'architecture centralisée

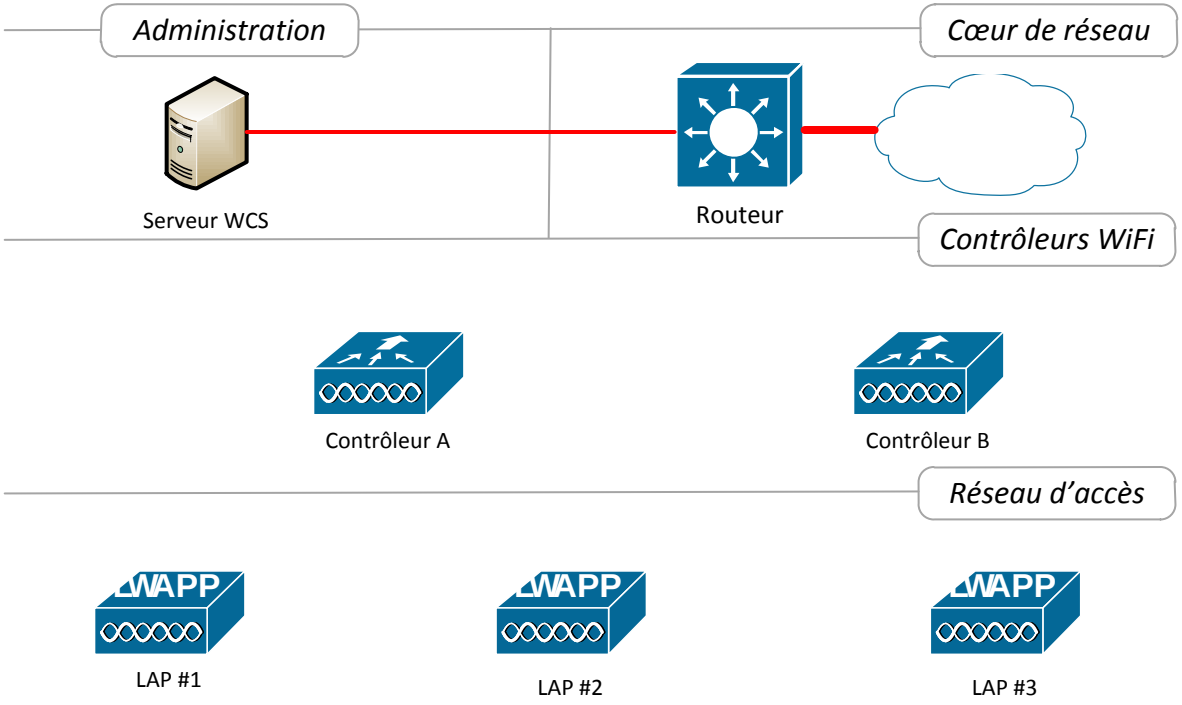


Schéma d'architecture centralisée

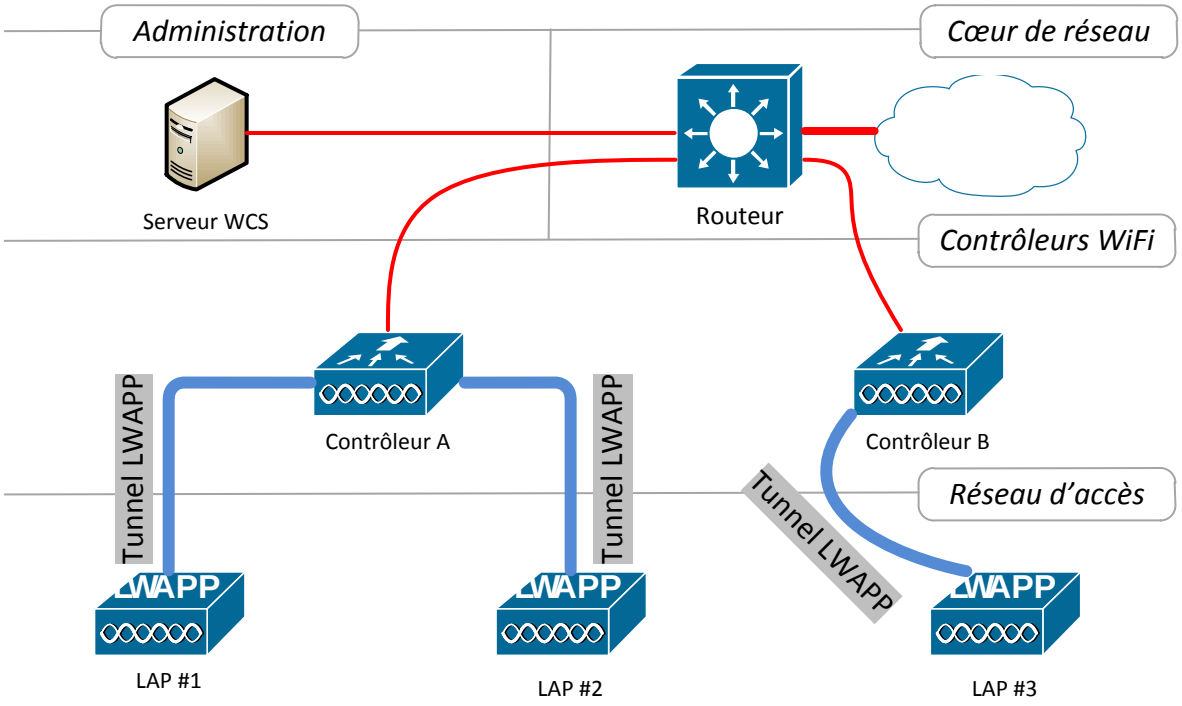
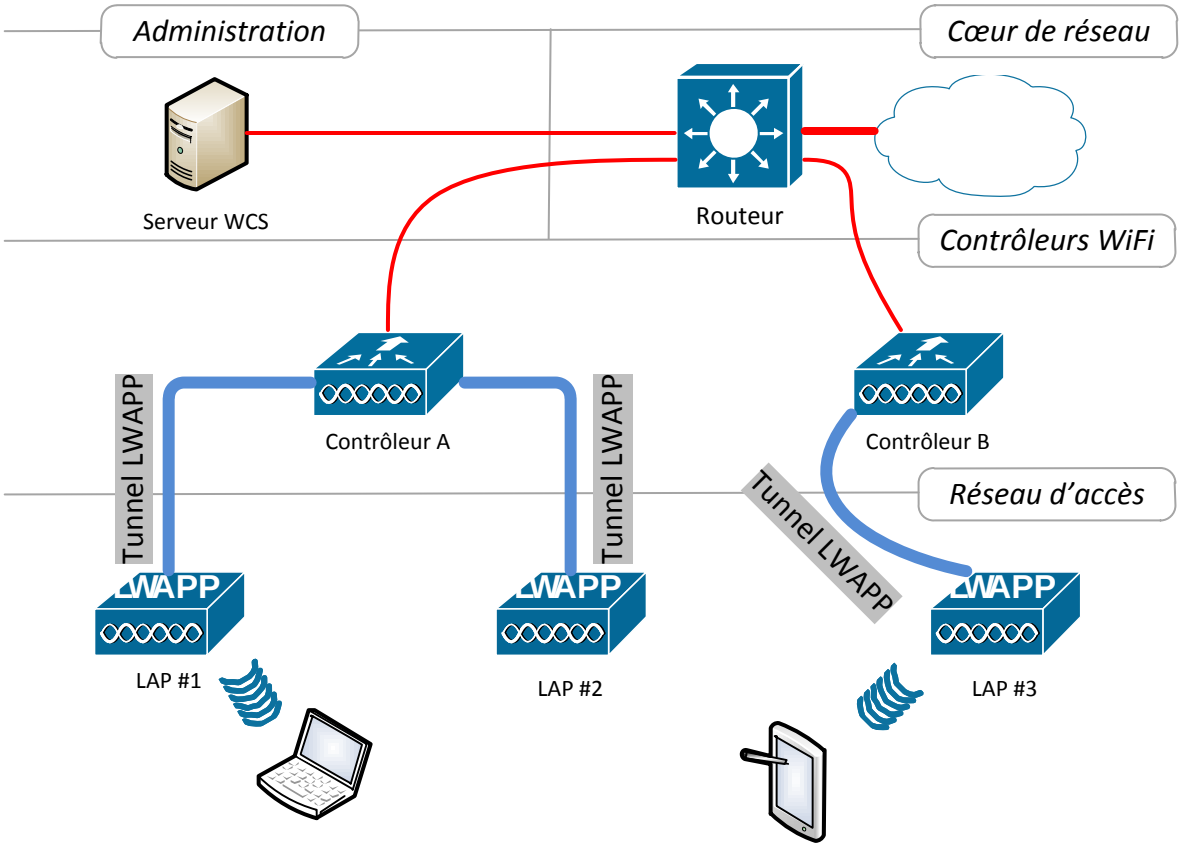


Schéma d'architecture centralisée



Point d'accès léger

- « Léger » car assurent les fonctions de base du sans-fil:
  - Couche physique (DSSS, OFDM, MIMO, …)
  - Une partie de la couche liaison:
    - CSMA/CA
    - Balises de signalisation *(beacons)*
    - Chiffrement de niveau 2 *(WPA et al.)*
    - Buffers de transmission/réception
    - Files QoS
    - Encapsulation/décapsulation LWAPP, fragmentation
  - Les fonctions avancées de la couche liaison sont déportées au contrôleur:
    - Associations 802.11
    - Gestion du chiffrement (définition des politiques de sécurité, *authenticator* EAP)
    - Etc.

Découverte des contrôleurs

- Comment l'AP se rattache-t-il à son contrôleur de gestion ?

- Deux étapes:
  1. Etablissement d'une liste de candidats:
     - Découverte par *broadcast* sur le réseau local
     - DHCP (champ *TLV* dans la réponse DHCP)
     - Requête DNS
     - Préconfiguration en dur
  2. Sélection parmi cette liste
     - Contact de chaque contrôleur (unicast) pour récupérer le statut
     - Requête d'enregistrement « JOIN », fonction de plusieurs critères (dont la charge en AP)

LAP, un matériel particulier ?

- Chez Cisco, les LAP sont des matériels classiques
  - Seul le micrologiciel *(firmware)* change
  - Bascule entre AP lourd et LAP par simple flashage
    - Opération réversible
  - Exemple de modèles:
    - Cisco AIRONET AP-1120, AP-1130, AP-1140, AP-1240




Contrôleur

- On parle de WLC *(Wireless Lan Controller)*, c'est le cerveau de l'architecture centralisée

- Pilote les bornes:
  - Gestion des versions logicielles et configurations
  - Politiques de sécurité
  - Gestion des RF
  - QoS

- Fonctionnalités avancées:
  - Mobilité
  - IPS/IDS
  - Cache DHCP/RADIUS

- Point de sortie de tout le trafic LWAPP client, relié au réseau entreprise

Contrôleur

- Large gamme, différentes capacités:

WLC	Capacité (AP)
2100 series	6 / 12 / 25
4402	12 / 25 / 50
4404	100
5508	250
WiSM	300

Serveur de gestion

- WCS *(Wireless Control System)*
- Se place au-dessus des contrôleurs
- Administration depuis un point unique
  - Peut gérer tout contrôleur joignable par IP, y compris donc au travers du WAN
- Interface Web
- Définition de *templates* de configuration, applicables aux contrôleurs et aux AP
  - SSID
  - Interfaces (VLAN, adresse), politique sans-fil (802.11 a/b/g/n)
  - Serveurs DHCP, RADIUS
  - Etc.

Avantages

- Gestion des configurations
  - Des versions de configurations homogènes
  - Configuration modifiée instantanément par le contrôleur (messages LWAPP)
  - Une seule interface de gestion (serveur WCS)

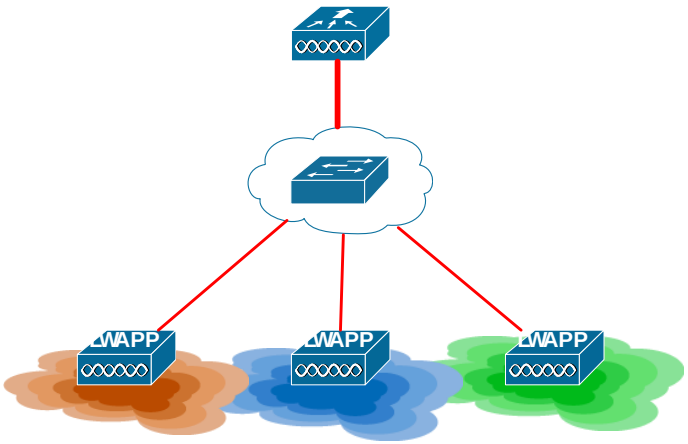
Avantages

- Facilités d'administration
  - Ajout d'un point d'accès:
    1. Propagation d'un seul VLAN dans le réseau local
    2. Connexion à un port d'accès
    3. Paramétrage IP (par DHCP le plus souvent)
    4. Puis configuration depuis le système WCS par application de *templates*

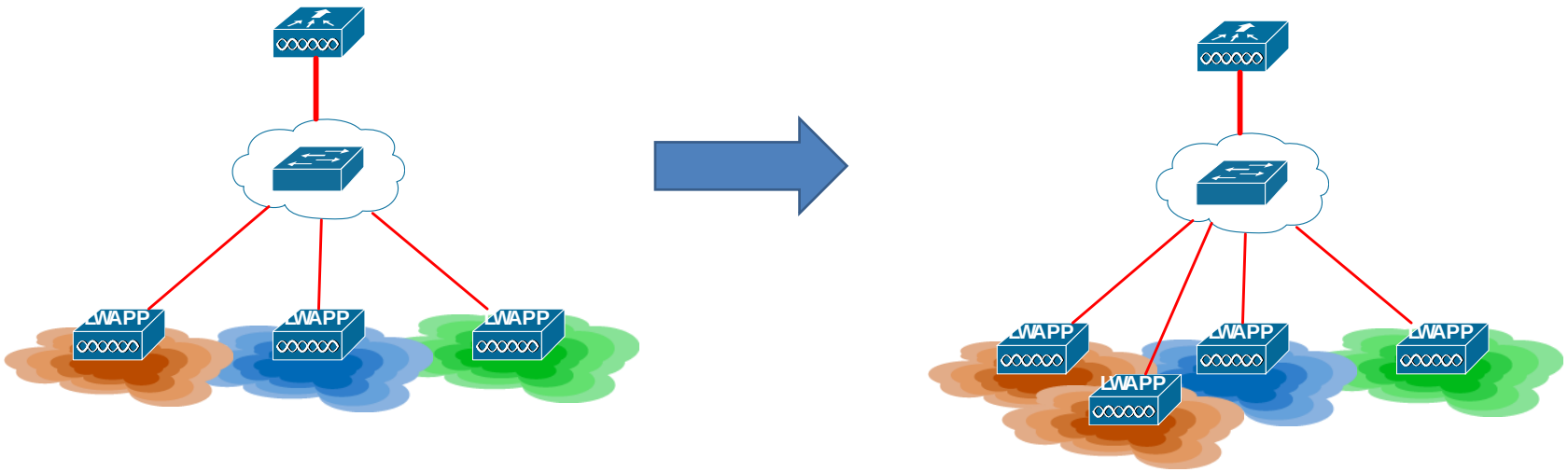
Gestion automatique des RF

- En 802.11b/g/n, seuls 3 canaux sont superposables
- Définir l'agencement pour un petit nombre d'AP est facile, mais cela peut vite se compliquer
  - Cas des bâtiments à plusieurs étages !
- Solution centralisée = visibilité sur un ensemble d'AP
  - Auto-configuration des paramètres RF (fréquence, puissance)
  - Ajustement en temps réel (réponse aux pannes ou interférences)
  - Equilibrage de charge pour les clients

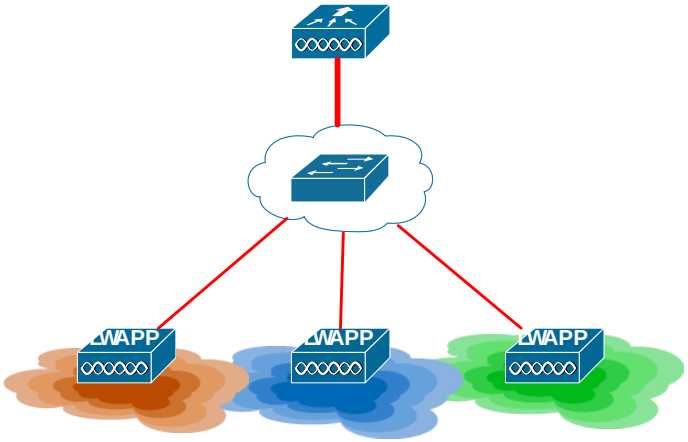
Réagencement automatique RF

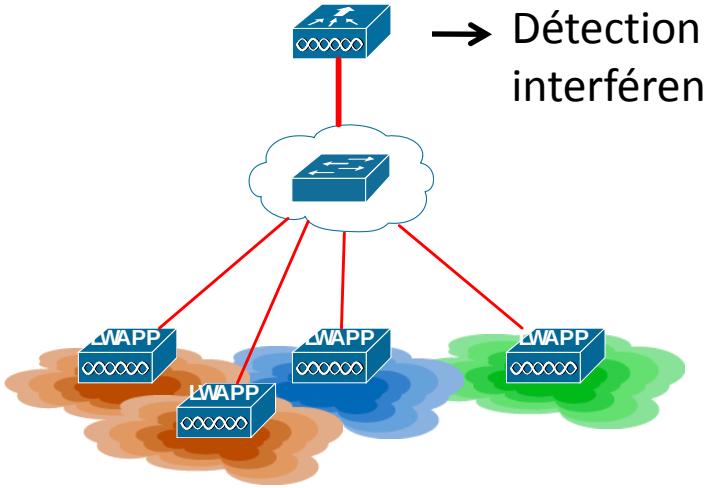


Réagencement automatique RF



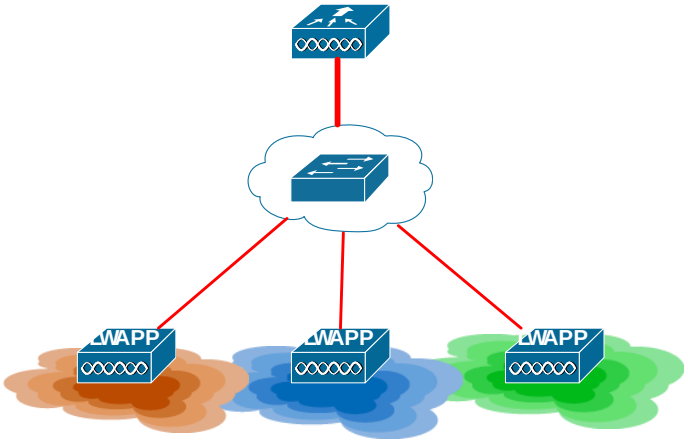
Réagencement automatique RF

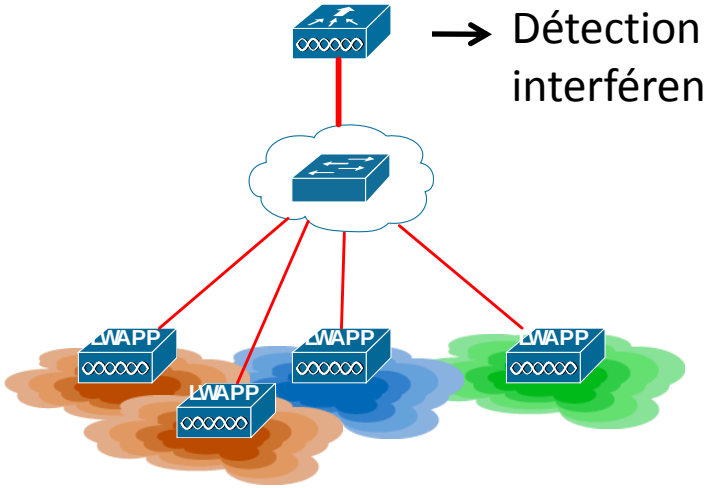




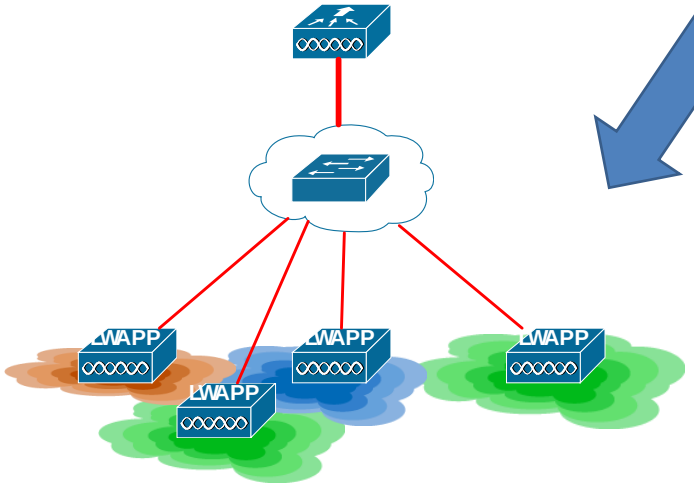
→ Détection des interférences

Réagencement automatique RF



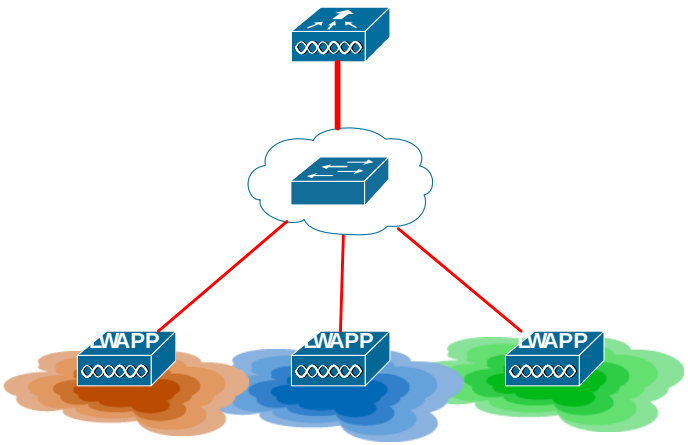


→ Détection des interférences

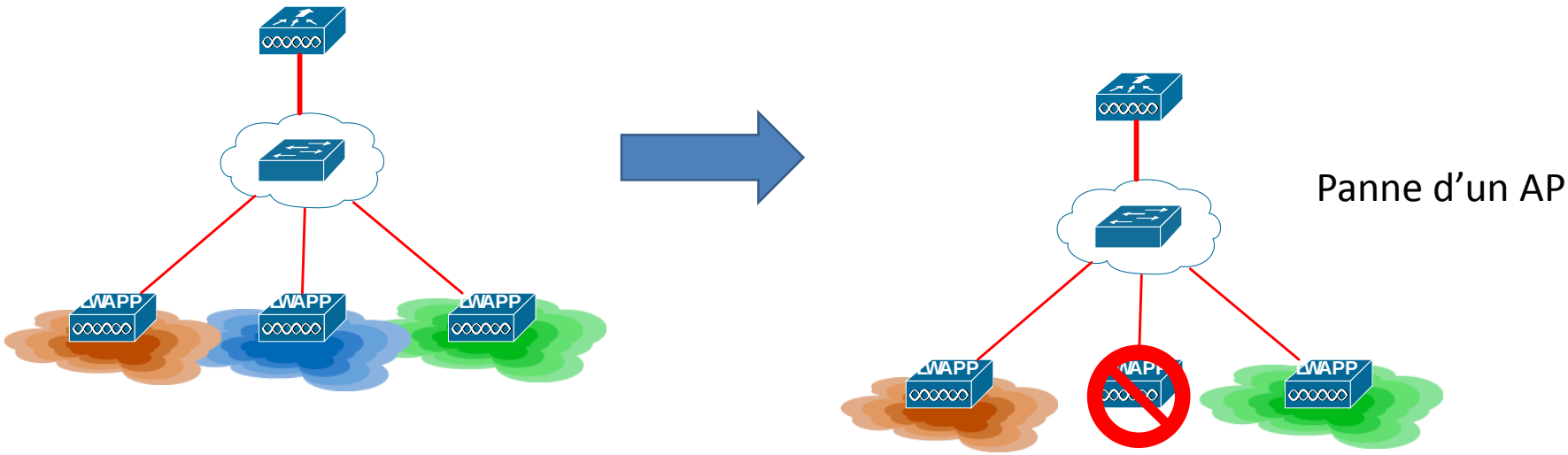


- Réagencement des canaux
- Diminution de la puissance d'émission

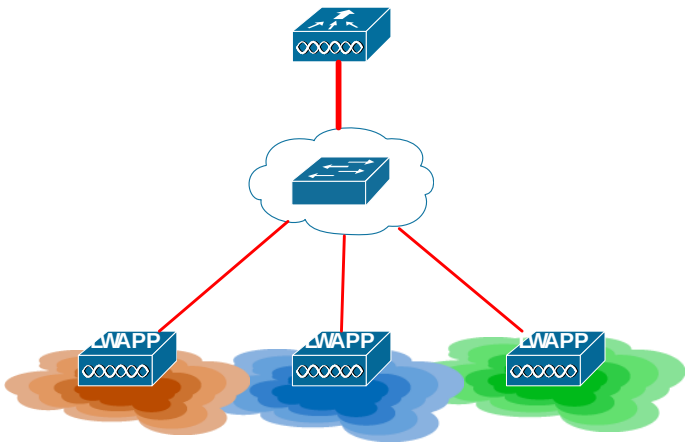
Ajustement automatique RF

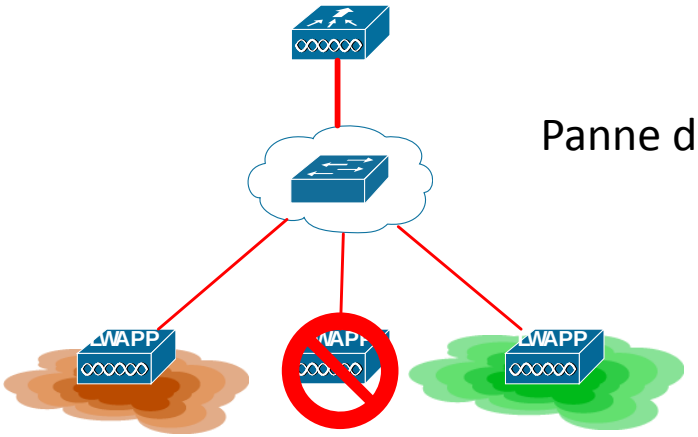


Ajustement automatique RF

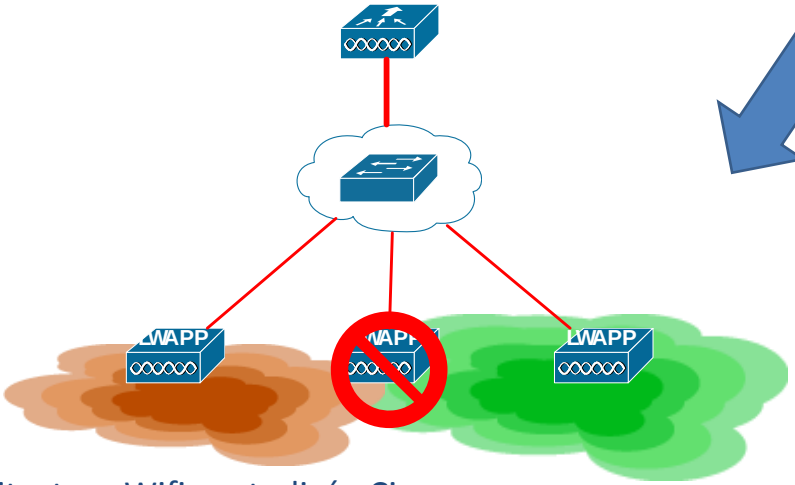


Ajustement automatique RF





Panne d'un AP



La puissance d'émission des deux AP est ajustée pour couvrir la zone

Bénéfices en sécurité

- Sécurisation des configurations et informations sensibles sur le contrôleur
- Une seule IP source pour le service RADIUS (réduit surface attaque)
- Détection et action coordonnées contre les éléments potentiellement dangereux
  - Rogue AP
    - Les AP peuvent envoyer des trames de désassociation au client qui tenterait de s'y associer
  - Rogue client
    - Possibilité de bannir de manière globale un client. Interdiction possible dès l'étape d'association!

Fonctionnalités avancées

- Mobilité:
  - Entre AP (niveau 2)
  - Entre contrôleurs (niveau 2/3)
- Handover/roaming mieux géré:
  - Vue globale du contrôleur sur les AP
  - Transfert et mise en cache des données utilisateur
  - Cache DHCP/RADIUS
- Fonctions de géolocalisation
  - Par tags RFID
  - Nécessite un *appliance* spécifique

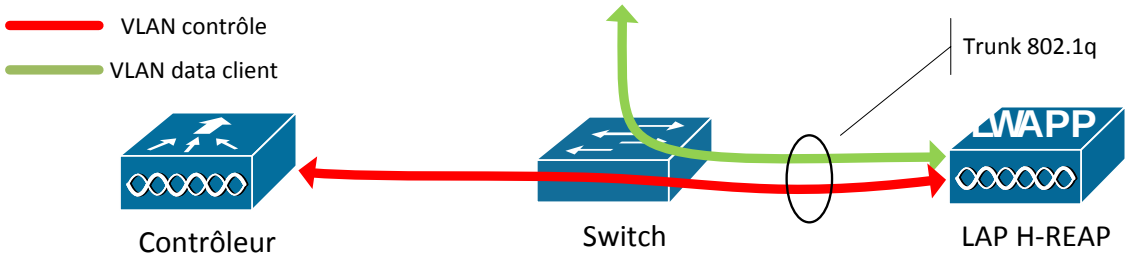
Inconvénients

- Le contrôleur est un point central, donc extrêmement critique
  - Attention à sa défaillance !

- Pour le contrôleur, deux types de solutions:
  - Résilience physique
    - Plusieurs ports d'uplink vers le cœur de réseau (agrégation de liens par *trunking*)
    - Double alimentation électrique systématique
  - Backup par utilisation d'autres contrôleurs
    - Locaux
    - Distants (attention à la latence !)

Inconvénients

- Pour les AP, possibilité d'une utilisation hybride (H-REAP):
  - Flux de contrôle remontés jusqu'au contrôleur
  - Flux client commutés localement au port de rattachement au LAN
    - Mais oblige à placer les AP sur des trunks 802.1q, ce qui est justement ce qu'on veut éviter



Inconvénients

- Le prix!
- Double facturation:
  - Matériels physiques
    - Prix des contrôleurs peut devenir élevé, notamment pour la solution WiSM
    - Nécessite un serveur pour la console d'administration
      - On peut utiliser une machine virtuelle
  - Licences d'utilisation (pour les AP)
    - Mais répartition flexible depuis la console d'administration

Sommaire

1. De quoi parle-t-on ?
2. Architecture autonome
3. Architecture centralisée
4. Protocole d'échange: LWAPP
5. Bibliographie

4. Protocole d'échange: LWAPP

- Protocole de transfert de données entre AP et contrôleurs
- Introduit en 2002 (Airespace, rachetée par Cisco depuis)
- Retenu comme base pour une standardisation par l'IETF pour le futur standard CAPWAP (2006)
- CAPWAP: RFC 5415 (*Proposed standard*, mars 2009)

Caractéristiques

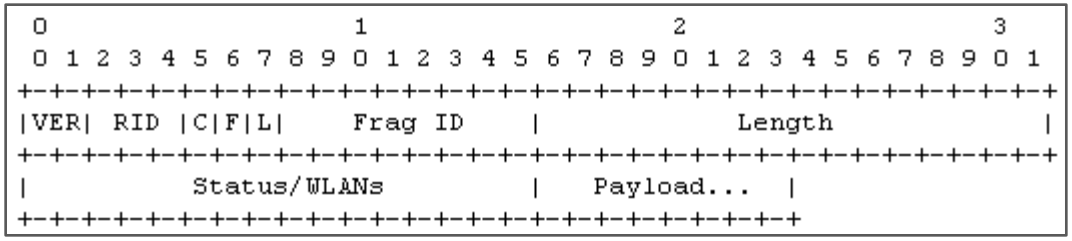
- Tunnel qui véhicule deux types de données:
  - Flux de contrôle (chiffrés)
  - Flux utilisateurs (en clair)
- Opère à deux niveaux, L2 ou L3:
  - L2: Au dessus d'Ethernet: Ethertype 0xBBBB
  - L3: Au-dessus d'IP, dans un datagramme UDP
- L2 est considéré comme obsolète:
  - Non routable
  - Oblige à une visibilité L2 entre contrôleur et LAP (même VLAN)
  - Non retenu dans CAPWAP

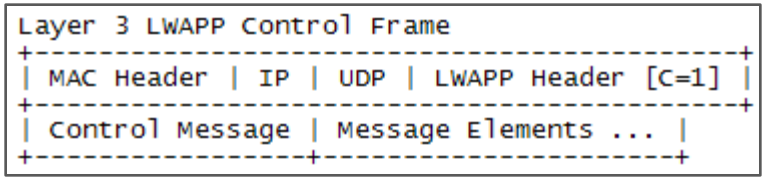
LWAPP Layer 3

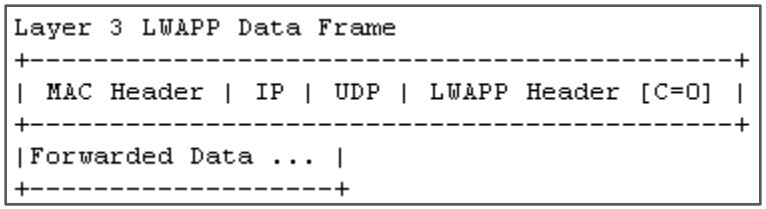
- Trafic encapsulé dans un datagramme UDP
  - Flux de contrôle: port destination 12223
    - Chiffré AES-CCM (chiffrement symétrique)
    - Utilise des certificats X.509 (AP et contrôleur)
      - Générés par la PKI Cisco à la fabrication
      - Stockés dans une mémoire flash protégée
  - Flux utilisateurs: port destination 12222
    - La totalité de la trame 802.11 est encapsulée
    - Dans CAPWAP, il est possible de n'encapsuler que la partie 802.3
- Le datagramme est envoyé en unicast au contrôleur (IP)

Format de trame

- Un en-tête LWAPP commun :







- La surcharge introduite par l'en-tête LWAPP est de 6 octets
  - Avec MAC + IP + UDP + LWAPP, total de 48 octets (3% du MTU)
  - Si fragmentation du paquet IP, pas de répétition de l'en-tête LWAPP

Conclusion

- Architecture apportant de nombreux bénéfices
  - Gestion plus simple/rationnelle du réseau
  - Apport de services

- Pertinence de s'équiper à évaluer en fonction du budget

Sommaire

1. De quoi parle-t-on ?
2. Architecture autonome
3. Architecture centralisée
4. Protocole d'échange: LWAPP
5. Bibliographie

Bibliographie

- Documentations officielles Cisco:
  - Général
    - http://snipurl.com/ciscocuw
  - Sécurisation X.509
    - http://snipurl.com/ciscox509
- Protocole CAPWAP: RFC 5415
    - http://snipurl.com/rfc5415
- Draft LWAPP
    - http://snipurl.com/draftlwapp
- Blog Infracom
    - http://infracom-france.com/blog2/?tag=lwapp

Questions ?