FC9RE09 **2 150 €** **3 jour(s)**

WiFi et réseaux sans fil – Concepts et mise en œuvre

OBJECTIFS

- Déployer le réseau WiFi en fonction des besoins domestiques ou industriels
- Appliquer les normes 802.11 et les spécifications techniques intégrées à la certification WiFi
- Déployer un réseau sans fil dans un bâtiment, comprendre les risques et mettre en place des mécanismes de sécurité.
- Appliquer la réglementation française et être sensibilisé au cadre international
- Analyser les causes impactant les performances d'un réseau WiFi
- Mettre en œuvre la qualité de service pour le transport de la voix

PROGRAMME

Introduction

- Principes généraux, architectures sans fil, problématique
- Positionnement de WiFi dans le panorama des réseaux sans fil et des autres techniques concurrentes

Propagation radio et caractéristiques du média

- Propagation radio indoor : défaut et contre-mesures, techniques de multiplexage, caractéristiques d'un récepteur

802.11 de b à ax, évolution des codages physiques

- Caractéristiques d'un signal numérique
- Introduction aux modulations sur fréquence porteuse
- DSSS et 802.11b
- OFDM et 802.11 a / g
- MIMO et 802.11 n / ac
- Nouveaux apports de 802.11ax,
- Wigig à 60 GHz – 802.11ad et ay
- Autres normes orientées couche physique
- Synthèses des différentes normes et performances

RÉALISABLE À DISTANCE

PANORAMA

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Ingénieurs et techniciens, responsables réseaux ou télécommunications, désirant déployer un réseau local sans fil ou souhaitant adjoindre une connexion locale sans fil à leurs réseaux existants.

Des connaissances de base sur les réseaux sont nécessaires pour suivre avec profit cette formation.

COORDINATEURS

Frédéric WEIS

Maître de conférence au département Télécom et Réseaux de l'IUT de Saint-Malo, il exerce ses activités de recherche à l'IRISA dans les domaines des applications mobiles et de l'informatique persuasive.

Laurent PARIZE

Il est Professeur agrégé à l'Université de Rennes 1 et enseignant au département Télécom et Réseaux de l'IUT de Saint-Malo.

MODALITES PEDAGOGIQUES

La formation comprend des

Architecture et tramage 802.11

- Modes de fonctionnement (adhoc, cellulaire, mesh, etc.)
- Structure de la couche MAC 802.11
- Technique d'accès DCF (CSMA/CA), notion de partage d'accès, limites
- Format des trames 802.11

Déploiement de systèmes sans fil WiFi

- Cadre légal
- État des connaissances de l'impact sur la santé
- Règles et conseils de déploiement
- Géolocalisation dans un bâtiment à l'aide de WiFi

Démonstrations radio

- Configuration radio d'un point d'accès
- Paramètres d'un client WiFi, tests de débit
- Outils d'aide au déploiement et à la supervision

WiFi et/ou 802.11 : quelles différences ?

- Principes du programme de certification WiFi
- Panorama des principales normes 802.11
- Panorama de la certification WiFi de la WiFi alliance
  - Tests obligatoires (radio, sécurité)
  - Procédures de configuration de sécurité (WPS, Passpoint et Easy Connect)
  - Exploitation des liens WiFi Direct dans un cadre domestique (Miracast, TDLS)
  - Exploitation de WiFi dans un cadre domestique (déploiement EasyMesh, TDLS, Miracast)

Sécurité d'un réseau WiFi : présentation des problématiques

- Problèmes de sécurité dans un réseau local sans fil
- Réseaux domestiques vs. réseaux d'entreprise : quelles différences
- Sécurisation d'un réseau WiFi public (HotSpot) : les problèmes à traiter

Sécurité intégrée dans WiFi : WPA/WPA2/WPA3

- SSID public ou SSID caché
- Problèmes traités : authentification et chiffrement
- Notions essentielles de cryptographie pour la sécurité WiFi
  - Faiblesses du chiffrement symétrique WEP
  - Chiffrements symétriques TKIP et AES
  - Hashage, chiffrement asymétrique/signature
  - Exploitation de certificats
- Mécanismes d'authentification : PSK et EAP/802.1x
- Différentes méthodes EAP : TLS, TTLS, PEAP, LEAP, SIM/AKA/AKA’

démonstrations en parallèle du cours, qui permettent de valider les notions abordées.

- WPA/WPA2 Personal et Enterprise, norme 802.11i ; la faille KRACK et l’évolution vers WPA3
- Déploiement d'un réseau multi-SSID et gestion des VLAN

Sécurisation d'un réseau WiFi public

- Problèmes posés par un réseau ouvert
- Sécurisation de l'accès par un portail captif : principes et limites
- Protection par réseaux privés virtuels (VPN)
- La spécification WiFi Passpoint (HotSpot 2.0), l’exploitation de WPA2 entreprise dans un réseau ouvert

Démonstrations sécurité WiFi

- Configuration d'un réseau WiFi ouvert
- Configuration multi SSID via une politique de VLAN
- Configuration d'un accès sécurisé via WPA2 PSK puis WPA2 entreprise (installation de certificats, configuration d'un serveur Radius puis authentification EAP-TLS)

Déploiement et administration d'un réseau WiFi étendu

- Des AP « lourds » aux AP « légers » : quels changements
- Notion de contrôleur WLC, principe de la configuration automatique des AP
- Principaux acteurs du marché
- État de la normalisation CAPWAP
- Fonctions avancées : IDS, RRM

VoWiFi (Voice Over WiFi) : principes généraux

- Problèmes à traiter : mobilité, qualité de service, sécurité
- État de la normalisation : 802.11r/k/i/e
- Qualité de service 802.11, la spécification WMM, les profils applicatifs WiFi Voice Personal et Voice Enterprise
- Gestion de la mobilité 802.11r, les interactions avec 802.11i, la gestion radio 802.11k
- Perspectives pour la VoWiFi

Synthèse et conclusion