PANORAMA | RÉALISABLE EN ANGLAIS | FAISABLE À DISTANCE

WIFI ET RÉSEAUX SANS FIL
CONCEPTS ET MISE EN ŒUVRE

FFCNCERCERXRE09 | PRIX : 2 580 € | DURÉE : 3 JOURS

Pauses et déjeuners offerts

PRÉSENTATION

La technologie Wi-Fi s'appuie sur une multitude de normes et de spécifications, et vise différents cadres fonctionnels et applicatifs.

La formation prend en compte les dernières évolutions de la certification Wi-Fi et aborde tous les aspects de la technologie Wi-Fi.

OBJECTIFS

- Déployer le réseau Wi-Fi en fonction des besoins domestiques ou industriels
- Appliquer les normes 802.11 et les spécifications techniques intégrées à la certification Wi-Fi
- Déployer un réseau sans fil dans un bâtiment
- Identifier 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 Wi-Fi
- Mettre en œuvre la qualité de service pour le transport de la voix

PROGRAMME

Propagation radio et caractéristiques du média 802.11

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

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

Wi-Fi et/ou 802.11 : quelles différences ?

Sécurité d'un réseau Wi-Fi public : présentation des problématiques
- Réseau local sans fil, réseaux domestiques vs. d'entreprise, réseau Wi-Fi public (HotSpot)

Sécurité intégrée : WPA/WPA2/WPA3
- SSID public ou SSID caché
- Problèmes traités : authentification et chiffrement
- Mécanismes d'authentification : PSK et EAP/802.1x
- Différentes méthodes EAP : TLS, TTLS, PEAP, LEAP, SIM/AKA/AKA
- 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 Wi-Fi public
- Sécurisation de l'accès par un réseau ouvert
- Sécurisation de l'accès par un portail captif : principes et limites
- Protection par réseaux privés virtuels (VPN)
- Spécification Wi-Fi Passpoint (HotSpot 2.0), l'exploitation de WPA2 entreprise dans un réseau ouvert

Démonstrations sécurité Wi-Fi
- Configurations réseau Wi-Fi ouvert, multi SSID via une politique VLAN

Déploiement et administration d'un réseau Wi-Fi étendu
- Notion de contrôleur WLC, principe de la configuration automatique des AP
- État de la normalisation CAPWAP et fonctions avancées : IDS, RRM

Vo Wi-Fi (Voice Over Wi-Fi)
- Qualité de service 802.11, spécification WMM, profils applicatifs Wi-Fi Voice Personal et Voice Enterprise
- Gestion de la mobilité 802.11r, interactions avec 802.11i, gestion radio 802.11k

Synthèse et conclusion

PUBLIC/PRÉREQUIS

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 en réseaux sont nécessaires afin de tirer pleinement profit de cette formation.

RESPONSABLE(S)

Frédéric WEIS
Enseignant-chercheur 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
Enseignant-chercheur, professeur agrégé à l'Université de Rennes 1 et enseignant au département Télécom et Réseaux de l'IUT de Saint-Malo. Il est spécialiste des réseaux sans fil.

MODALITÉS PÉDAGOGIQUES

La formation comprend des travaux pratiques et des démonstrations en parallèle du cours et qui permettent de valider les notions abordées