



Association
Des
Neticiens

RÉSEAUX SANS FIL ET WI-FI

À distance et synchrone



Durée :
3 jours ou 6 séances de 3h



Format :
Travaux Dirigés
Travaux Pratiques



Coût :
2400€ net de taxe / stagiaire
Déclaration d'activité n° 11756034475 enregistrée
auprès du préfet de région d'Ile-De-France.
Cet enregistrement ne vaut pas agrément de l'Etat,
selon l'article L. 6352-12 du Code du travail



Effectif minimum :
Formation mise en place
à partir de 5 participants

Contact :

Anna TEA
anna.tea@neticien.net
07 61 11 64 69

Michel TABOURET
michel.tabouret@neticien.net
07 66 07 20 38

www. formations-neticiens.net

 @ADN-Association des Neticiens

Objectifs :

- ✓ Déployer le réseau Wi-Fi en fonction des besoins professionnels.
- ✓ Appliquer les normes 802.11 et les spécifications techniques intégrées à la certification Wi-Fi.
- ✓ 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.
- ✓ Optimiser les performances d'un réseau WiFi.
- ✓ Mettre en oeuvre la qualité de service pour le transport de la voix.

Prérequis :

Connaissances de base sur les systèmes d'information (fonctionnement, etc.)
Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications

Contenu de la formation :

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

Architecture et tramage 802.11

Modes de fonctionnement (ad hoc, cellulaire, mesh, ...)
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
Etat 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

9h

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 : les tests obligatoires (radio, sécurité), les procédures de configuration de sécurité (WPS, Passpoint et Easy Connect), l'exploitation des liens WiFi Direct dans un cadre domestique (Miracast, TDLS)

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

Quelques notions essentielles de cryptographie pour la sécurité WiFi : les faiblesses du chiffrement symétrique WEP, les 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'

Au final ... 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 enterprise 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 enterprise (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

Etat de la normalisation CAPWAP

Fonctions avancées : IDS, RRM

VoWiFi (Voice Over WiFi) : principes généraux

Problèmes à traiter : mobilité, qualité de service, sécurité

Etat 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

