



1. Planning de travail et répartition des tâches

Tâches +			
☀	Aa Nom	☰ Participants	📅 Date d'échéance
☐	<u>Documentation et apprentissage RADIUS, borne Wi-Fi Cisco</u>	Ugo Bernard Bruno Levesque	11 décembre 2024
☐	<u>Configuration de la borne Wi-Fi</u>	Bruno Levesque Ugo Bernard	13 décembre 2024
☐	<u>Configuration de RADIUS</u>	Ugo Bernard Bruno Levesque	20 décembre 2024
☐	<u>Procédure d'installation et de configuration de RADIUS</u>	Bruno Levesque	8 janvier 2025
☐	<u>Procédure de configuration de la borne Wi-Fi</u>	Ugo Bernard	8 janvier 2025

2. Présentation de la norme IEEE802.11

La norme IEEE 802.11, aussi connue sous le nom de Wi-Fi, est une famille de normes développée par l'Institute of Electrical and Electronics Engineers (IEEE) pour régir les communications sans fil locales (WLAN, Wireless Local Area Networks). Elle définit les spécifications techniques pour les réseaux sans fil permettant à divers appareils de se connecter à un réseau via des ondes radio.

2.1. Principes de base de la norme IEEE 802.11 :

Architecture réseau

- Mode infrastructure : Un point d'accès (AP, Access Point) agit comme une passerelle entre les périphériques sans fil et le réseau filaire.
- Mode ad hoc : Les périphériques communiquent directement entre eux sans point d'accès centralisé.



Bandes de fréquences

La norme IEEE 802.11 exploite principalement les bandes de fréquence 2,4 GHz et 5 GHz. Certaines extensions plus récentes incluent également la bande 6 GHz.

Sécurité

Les mécanismes de sécurité incluent les protocoles WEP, WPA, WPA2, et WPA3 pour garantir la confidentialité et la protection des données transmises.

Accès au canal

L'accès est géré par le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour minimiser les collisions entre les transmissions.

Versions et évolutions de la norme IEEE 802.11

Depuis sa première version en 1997, la norme IEEE 802.11 a évolué pour répondre aux besoins croissants en termes de débit, de portée, de densité des réseaux, et de fiabilité.

Voici les principales versions :

802.11 (1997) : Première version avec un débit maximum de 2 Mbps, désormais obsolète.

802.11a (1999) : Fonctionne en 5 GHz avec un débit maximum théorique de 54 Mbps.

802.11b (1999) : Fonctionne en 2,4 GHz avec un débit jusqu'à 11 Mbps.

802.11g (2003) : Fonctionne en 2,4 GHz avec un débit jusqu'à 54 Mbps.

802.11n (2009) : Utilisation des technologies MIMO (Multiple Input, Multiple Output), débit jusqu'à 600 Mbps, bandes 2,4 GHz et 5 GHz.

802.11ac (2013) : Fonctionne en 5 GHz, introduit MU-MIMO (Multi-User MIMO), débit jusqu'à 6,9 Gbps.

802.11ax (Wi-Fi 6, 2019) : Fonctionne en 2,4 GHz, 5 GHz, et 6 GHz (avec Wi-Fi 6E), utilise la modulation OFDMA pour une meilleure efficacité dans les environnements denses, débit jusqu'à 9,6 Gbps.

802.11be (Wi-Fi 7, en développement) : Débit prévu dépassant 30 Gbps grâce à des canaux plus larges (320 MHz) et des technologies avancées comme MLO (Multi-Link Operation).



Caractéristiques principales :

Interopérabilité

Les normes IEEE 802.11 garantissent une interopérabilité entre les équipements de différents fabricants certifiés par la Wi-Fi Alliance.

Portée

Varie en fonction des conditions environnementales et des bandes utilisées (environ 30 à 90 mètres en intérieur pour 2,4 GHz).

Applications

Réseaux domestiques, réseaux d'entreprise, lieux publics (hôtels, cafés, aéroports), et IoT (Internet des objets).

Conclusion

IEEE 802.11 est une norme essentielle pour les communications sans fil modernes. Ses évolutions successives répondent aux besoins croissants en termes de vitesse, d'efficacité et de sécurité, rendant le Wi-Fi omniprésent dans les environnements personnels et professionnels.

3. Etude comparative des différents protocoles de sécurité WIFI

3.1. Comparaison synthétique des protocoles

Protocole	Algorithme de chiffrement	Points forts	Points faibles	Statut actuel
WEP	RC4	Simple, universel à l'époque	Très faible sécurité, facilement cassable	Obsolète
WPA	RC4 + TKIP	Amélioration de WEP, dynamique	Vulnérable aux attaques modernes	Dépassé
WPA2	AES	Sécurisé, largement adopté	Failles comme KRACK	Standard courant
WPA3	AES + SAE	Très sécurisé, protection des réseaux ouverts	Compatibilité limitée	Standard recommandé