

TIP 3.5

Configurer un réseau Wi-Fi et ses protections

Fiche de révision - Module Infrastructure TIP

1. Architecture Wi-Fi

Client Wi-Fi → point d'accès → switch → réseau de l'entreprise
Une borne Wi-Fi relie le réseau radio au réseau Ethernet. Elle n'est pas forcément un routeur.

2. SSID et segmentation

Élément	À retenir
SSID	Nom logique du réseau Wi-Fi présenté au client.
Plusieurs SSID	Une même borne peut diffuser plusieurs réseaux Wi-Fi.
VLAN	Un SSID peut être associé à un réseau logique distinct.
Réseau invité	Doit généralement être isolé des ressources internes.

3. Bandes de fréquences

Bande	Avantages	Limites
2,4 GHz	Portée souvent meilleure, compatibilité large.	Bande très utilisée, davantage d'encombrement.
5 GHz	Débits souvent supérieurs, davantage de canaux.	Portée parfois moindre.
6 GHz	Disponible sur certains matériels récents.	Nécessite compatibilité et cadre réglementaire adapté.

4. Canaux et largeur de canal

Les réseaux Wi-Fi partagent un spectre radio divisé en canaux. Des bornes trop proches sur des canaux mal choisis peuvent se perturber. Des largeurs de 20, 40 ou 80 MHz existent selon le contexte : plus large peut offrir plus de débit, mais consomme davantage de spectre.

5. Générations Wi-Fi

Désignation	Norme
Wi-Fi 4	802.11n
Wi-Fi 5	802.11ac
Wi-Fi 6	802.11ax

6. Sécurité Wi-Fi

Mécanisme	À retenir
WEP	Obsolète et insuffisant.
WPA2	Encore largement rencontré.
WPA3	Génération plus récente, à privilégier lorsque l'environnement le permet.
Personal	Clé/phrase secrète partagée.
Enterprise	Authentification individuelle, souvent via 802.1X/RADIUS.

7. 802.1X et RADIUS

Schéma simplifié : client → point d'accès → serveur RADIUS → annuaire/politique → autorisation ou refus.
Dans un environnement Microsoft, NPS peut assurer le rôle de serveur RADIUS.

8. Mesures complémentaires

Mesure	Limite / usage
Filtrage MAC	Contrôle complémentaire ; ne remplace pas WPA2/WPA3.
SSID masqué	Ne constitue pas une protection forte à lui seul.
Isolation clients	Peut limiter les communications entre clients sur un réseau invité.
Portail captif	Peut contrôler l'accès invité, mais ne remplace pas les protections du réseau.

9. Connexion Wi-Fi ≠ accès réseau complet

Étape	Question de diagnostic
1. Détection	Le SSID est-il visible ?
2. Authentification	La clé, les identifiants ou le certificat sont-ils valides ?
3. Association	Le client est-il réellement connecté à la borne ?
4. DHCP	Une adresse IP correcte a-t-elle été reçue ?
5. Ressources	Passerelle, DNS et services sont-ils accessibles ?

10. Commandes Windows utiles

Commande	Utilité
Get-NetAdapter	État et vitesse des interfaces réseau.
netsh wlan show interfaces	SSID, BSSID, type radio, canal, signal et débit de liaison.
netsh wlan show networks mode=bssid	Réseaux détectés, BSSID, canaux et signaux.
netsh wlan show profiles	Profils Wi-Fi enregistrés sur Windows.
netsh wlan delete profile name="SSID"	Supprimer un profil Wi-Fi enregistré.
ipconfig /all	Vérifier IP, DHCP, passerelle et DNS après association.

11. Symptômes fréquents

Symptôme	Piste
SSID invisible	Carte Wi-Fi, portée, borne, bande de fréquence, diffusion/configuration.
Authentification impossible	Clé, identifiants, certificat, RADIUS, compatibilité WPA.
169.254.x.x	Association possiblement réussie, mais DHCP ou VLAN à examiner.
IP correcte, pas d'Internet	Passerelle, DNS, routage, pare-feu et accès opérateur.
Signal faible	Distance, obstacles, interférences, implantation des bornes.

12. Méthode de diagnostic

Ordre conseillé :
Carte Wi-Fi → SSID → signal → authentification → association → adresse IP → passerelle → DNS → ressource demandée.

13. À retenir

SSID : nom logique du Wi-Fi. 2,4 GHz : meilleure portée en général. 5 GHz : débits souvent supérieurs. WEP : obsolète. WPA2/WPA3 : protections modernes. 802.1X/RADIUS : authentification centralisée. Filtrage MAC et SSID masqué : mesures complémentaires seulement. Wi-Fi invité : à isoler du réseau interne. 169.254.x.x : penser DHCP/VLAN. Réflexe : radio → authentification → association → IP → DNS → ressources.