DOCUMENTATION TECHNIQUE

Configuration Borne Wi-Fi en Authentification RADIUS

SSID	Wifi_Techniciens
IP Borne Wi-Fi	172.20.3.4
IP Serveur RADIUS	172.20.1.74
Secret RADIUS	Bts2026$
Protocole	WPA2-Enterprise / EAP / AES

1. Présentation de l'architecture

Cette documentation décrit la configuration d'une borne Wi-Fi Cisco (série Aironet) en mode authentification centralisée via un serveur RADIUS (Remote Authentication Dial-In User Service) hébergé sur Windows Server.

L'authentification WPA2-Enterprise permet de ne pas partager une clé Wi-Fi commune à tous les utilisateurs. Chaque technicien s'authentifie avec ses propres identifiants Active Directory, ce qui renforce la traçabilité et la sécurité du réseau.

1.1 Schéma logique simplifié

[Client Wi-Fi Technicien]

↓ Association Wi-Fi (SSID : Wifi_Techniciens)

[Borne Wi-Fi Cisco — 172.20.3.4]

↓ RADIUS (UDP 1812/1813) — Secret : Bts2026$

[Windows Server NPS/RADIUS — 172.20.1.74]

2. Prérequis

Avant d'appliquer la configuration, vérifier que les éléments suivants sont en place :

- ✓ Le service NPS (Network Policy Server) est installé et démarré sur Windows Server (172.20.1.74)
- ✓ La borne Cisco est joignable en SSH ou console
- ✓ Les ports UDP 1812 (authentification) et 1813 (accounting) sont ouverts entre la borne et le serveur
- ✓ Un client RADIUS est déclaré dans NPS avec l'IP de la borne (172.20.3.4) et le secret partagé Bts2026$
- ✓ Une stratégie réseau NPS est créée pour autoriser le groupe de techniciens AD

3. Configuration de la borne Wi-Fi

La configuration s'effectue en mode CLI (Command Line Interface) depuis la console ou en SSH. Les étapes sont présentées dans l'ordre d'exécution recommandé.

Étape 1 — Création du SSID et paramètres d'authentification

Définir le SSID et activer l'authentification EAP (Extensible Authentication Protocol) requise pour WPA2-Enterprise.

```
AP(config)# dot11 ssid Wifi_Techniciens
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2
AP(config-ssid)# guest-mode
AP(config-ssid)# exit
```

Commande	Rôle
dot11 ssid Wifi_Techniciens	Crée le profil SSID
authentication open eap eap_methods	Autorise le trafic ouvert conditionné à l'EAP
authentication network-eap eap_methods	Oblige l'authentification EAP sur le réseau
authentication key-management wpa version 2	Force le chiffrement WPA2
guest-mode	Diffuse le SSID en mode visible (beacon)

Étape 2 — Activation du modèle AAA

Activer le framework AAA (Authentication, Authorization, Accounting) sur la borne, nécessaire pour déléguer l'authentification à un serveur externe.

```
AP(config)# aaa new-model
```

⚠ Cette commande est indispensable. Sans elle, la borne ne peut pas contacter de serveur RADIUS externe. Elle doit être saisie avant toute configuration AAA.

Étape 3 — Déclaration du serveur RADIUS

Indiquer à la borne l'adresse IP du serveur RADIUS, les ports d'écoute ainsi que le secret partagé.

```
AP(config)# radius-server host 172.20.1.74 auth-port 1812 acct-port 1813 key
Bts2026$
```

Paramètre	Valeur
Adresse IP serveur RADIUS	172.20.1.74 (Windows Server NPS)
Port authentification	1812 (UDP — standard RADIUS)
Port accounting	1813 (UDP — standard RADIUS)
Secret partagé (key)	Bts2026$

Étape 4 — Création du groupe de serveurs RADIUS

Regrouper le serveur RADIUS dans un groupe logique qui sera référencé dans la méthode d'authentification.

```
AP(config)# aaa group server radius RADIUS_GROUP
AP(config-sg-radius)# server 172.20.1.74 auth-port 1812 acct-port 1813
AP(config-sg-radius)# exit
```

Étape 5 — Liaison de la méthode d'authentification EAP

Associer la liste de méthodes eap_methods (référencée dans la config SSID) au groupe RADIUS_GROUP.

```
AP(config)# aaa authentication login eap_methods group RADIUS_GROUP
```

Étape 6 — Configuration de l'interface radio

Appliquer le SSID et le mode de chiffrement AES sur l'interface radio dot11Radio 0 (Wi-Fi 2,4 GHz).

```
AP(config)# interface dot11Radio 0
AP(config-if)# ssid Wifi_Techniciens
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# exit
```

⚠ aes-ccm correspond à l'algorithme AES en mode CCM (Counter with CBC-MAC), le chiffrement utilisé par WPA2. C'est le standard recommandé pour la sécurité des réseaux Wi-Fi d'entreprise.

4. Configuration complète — Récapitulatif

Voici l'intégralité des commandes à saisir dans l'ordre, prêtes à copier-coller dans la console de la borne :

```
! ── SSID & Authentification EAP ──
AP(config)# dot11 ssid Wifi_Techniciens
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2
AP(config-ssid)# guest-mode
AP(config-ssid)# exit
!
! ── Activation AAA ──
AP(config)# aaa new-model
!
! ── Serveur RADIUS (Windows Server NPS) ──
AP(config)# radius-server host 172.20.1.74 auth-port 1812 acct-port 1813 key
Bts2026$
!
! ── Groupe RADIUS ──
AP(config)# aaa group server radius RADIUS_GROUP
AP(config-sg-radius)# server 172.20.1.74 auth-port 1812 acct-port 1813
AP(config-sg-radius)# exit
!
! ── Méthode d'authentification EAP -> RADIUS_GROUP ──
AP(config)# aaa authentication login eap_methods group RADIUS_GROUP
!
! ── Interface radio 2,4 GHz ──
AP(config)# interface dot11Radio 0
AP(config-if)# ssid Wifi_Techniciens
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# exit
!
! ── Sauvegarde ──
AP# write memory
```

5. Vérification et dépannage

5.1 Commandes de vérification

```
AP# show radius statistics    ! Statistiques RADIUS
AP# show aaa servers           ! Configuration AAA
AP# show dot11 associations    ! Clients Wi-Fi associés
AP# show dot11 ssid            ! Configuration du SSID
AP# show running-config        ! Configuration complète
```

5.2 Problèmes fréquents

Symptôme	Solution
Le client ne peut pas s'authentifier	Vérifier que le secret Bts2026$ est identique sur la borne ET dans NPS
Timeout RADIUS	Contrôler que les ports UDP 1812/1813 sont ouverts sur le firewall Windows Server
SSID non visible	Vérifier que guest-mode est bien configuré sur le SSID
Erreur 'invalid key'	Re-saisir la commande radius-server host avec le secret exact (attention à la casse)
Association refusée	Vérifier la stratégie réseau NPS : le groupe AD doit être autorisé