Conception et déploiement d'une infrastructure réseau sécurisée

Réponse à l'appel d'offre — Campus Mediaschool IRIS Nice

Auteur : Nedjmeddine Belloum — BTS SIO option SISR

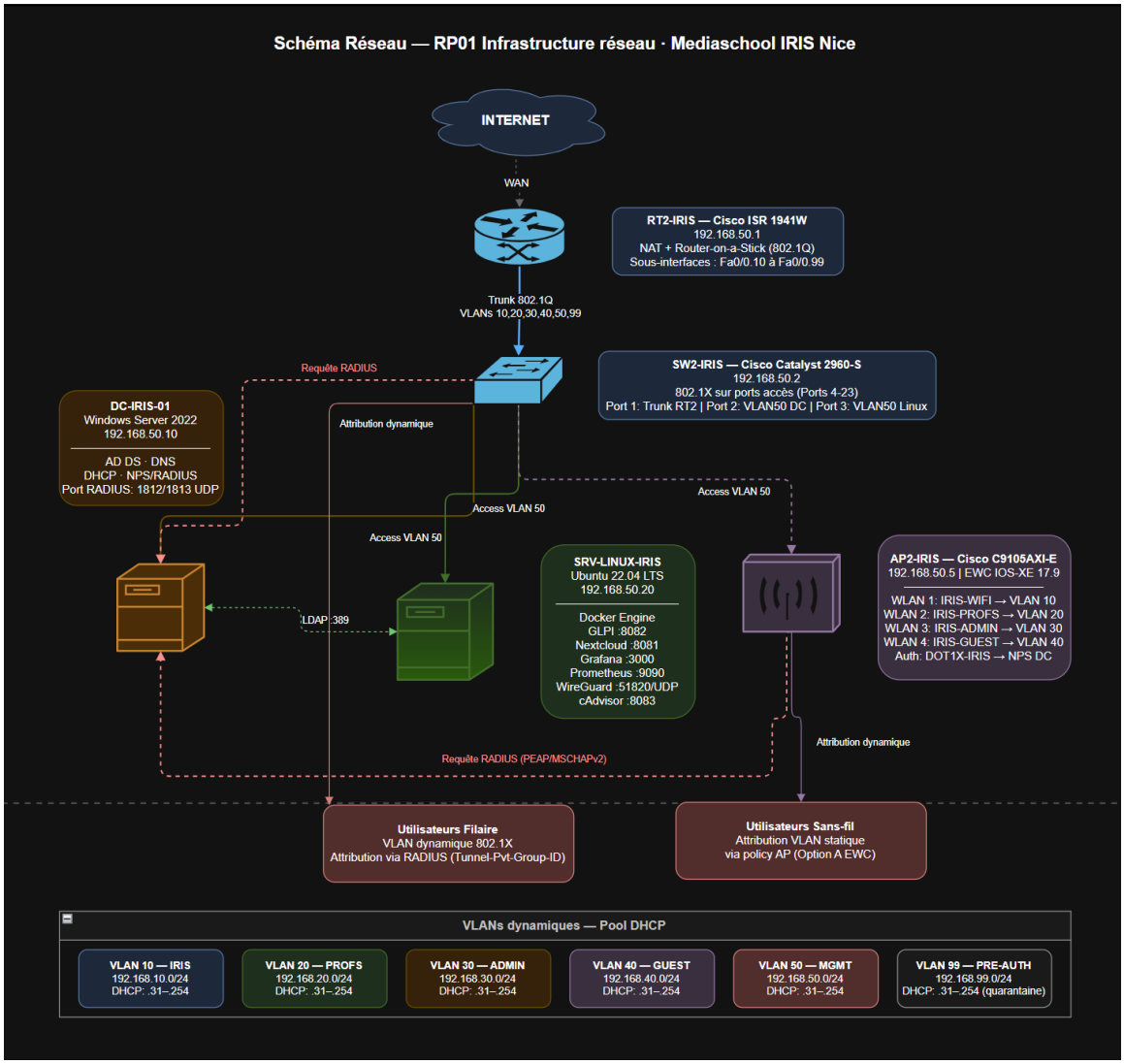
Établissement : MEDIASCHOOL Nice

1. Contexte et objectif du projet

Réponse à l'appel d'offre du campus Mediaschool pour la conception et le déploiement d'une infrastructure réseau segmentée, sécurisée et supervisée. L'ensemble des solutions retenues est 100 % open source (hors équipements Cisco fournis). Le projet couvre l'authentification réseau IEEE 802.1X/RADIUS, la gestion centralisée Active Directory, le WiFi sécurisé WPA2-Enterprise et la supervision Prometheus/Grafana.

Besoin exprimé	**Solution retenue**	**Statut**
Segmentation réseau par VLAN	6 VLANs — Cisco SW2-IRIS Catalyst 2960-S	Validé
Authentification réseau 802.1X	NPS/RADIUS sur DC-IRIS-01 Windows Server 2022	Validé
Gestion centralisée utilisateurs	Active Directory DS + FGPP + GPO	Validé
WiFi WPA2-Enterprise	AP Cisco C9105AXI-E (EWC 17.9.8.5) — Option A	Validé
PKI interne	ADCS — CA racine IRIS-Root-CA sur DC-IRIS-01	Validé
Services applicatifs	Docker sur SRV-LINUX-IRIS Ubuntu 22.04 — 8 services	Validé
Supervision infrastructure	Prometheus + Grafana + Alertmanager	Validé
Isolation postes invités	VLAN 99 — Quarantaine — accès Internet uniquement	Validé

2. Architecture Générale



2.1 Inventaire des équipements

Équipement	Modèle	IP	Rôle
RT2-IRIS	Cisco ISR 1941W	192.168.50.1	Routeur — Passerelle inter-VLAN — NAT
SW2-IRIS	Cisco Catalyst 2960-S	192.168.50.2	Switch L3 — Trunk — 802.1X
AP2-IRIS	Cisco C9105AXI-E (EWC 17.9.8.5)	192.168.50.3	Point d'accès WiFi — WPA2-Enterprise
DC-IRIS-01	Windows Server 2022 Standard	192.168.50.10	AD DS — NPS/RADIUS — DHCP — PKI
SRV-LINUX-IRIS	Ubuntu Server 22.04 LTS + Docker	192.168.50.20	Services applicatifs — 8 conteneurs

2.2 Plan d'adressage VLAN

VLAN	Réseau	Nom	Portée DHCP	Utilisation

VLAN 10	192.168.10.0/24	ETUDIANTS	192.168.10.100–200	Postes étudiants — authentification 802.1X
VLAN 20	192.168.20.0/24	PROFS	192.168.20.100–150	Postes professeurs — authentification 802.1X
VLAN 30	192.168.30.0/24	ADMIN	192.168.30.100–120	Administration — accès complet
VLAN 40	192.168.40.0/24	SERVERS	Statique	Serveurs (DC-IRIS-01 + SRV-LINUX-IRIS)
VLAN 50	192.168.50.0/24	MANAGEMENT	Statique	Équipements réseau (RT2, SW2, AP2)
VLAN 99	192.168.99.0/24	QUARANTAINE	192.168.99.100–200	Postes non conformes — Internet uniquement

3. Équipements Cisco

3.1 RT2-IRIS — Cisco ISR 1941W

Paramètre	Valeur
Modèle	Cisco ISR 1941W
IP Management	192.168.50.1 — VLAN 50
Rôle	Routeur — Passerelle inter-VLAN — NAT vers Internet
Interfaces	Fa0/0 WAN (DHCP) — Fa0/1 LAN trunk vers SW2-IRIS
Sous-interfaces	Fa0/1.10 à .20 à .30 à .40 à .50 à .99 (encapsulation dot1Q)
ACL	DENY VLAN99 vers réseaux internes — PERMIT tout autre
SSH	Version 2 — timeout 60s — retries 3
Secret enable	Cisco123! (haché MD5 type 5)

3.2 SW2-IRIS — Cisco Catalyst 2960-S

Paramètre	Valeur
Modèle	Cisco Catalyst 2960-S 24 ports
IP Management	192.168.50.2 — VLAN 50
Rôle	Switch L3 — Trunk — Authentification 802.1X par port
802.1X	dot1x system-auth-control — aaa authentication dot1x
NPS/RADIUS	192.168.50.10 — clé IrisRadius2026!
Uplink	Gi0/1 trunk vers RT2-IRIS (allowed VLAN 10,20,30,40,50,99)
Port access	VLAN assigné dynamiquement par RADIUS (Tunnel-Pvt-Group-ID)
VLAN auth fail	VLAN 99 — Quarantaine automatique si échec auth
Spanning Tree	PVST+ — PortFast sur ports accès

3.3 AP2-IRIS — Cisco C9105AXI-E (EWC 17.9.8.5)

Paramètre	Valeur
Modèle	Cisco Catalyst 9105AXI-E — EWC (Embedded Wireless Controller) v17.9.8.5

IP Management	192.168.50.3 — VLAN 50
Mode WiFi	Option A — VLAN statique par SSID (sans aaa-override)
SSID IRIS-ETUDIANTS	WPA2-Enterprise — VLAN 10 statique — AES/CCMP
SSID IRIS-PROFS	WPA2-Enterprise — VLAN 20 statique — AES/CCMP
SSID IRIS-INVITES	WPA2-Personal (PSK) — VLAN 99 — accès Internet uniquement
Authentification 802.1X	RADIUS vers DC-IRIS-01 (192.168.50.10:1812)
Raison Option A	EWC 17.9.8.5 incompatible avec aaa-override + FlexConnect local switching
Norme	IEEE 802.11i — PEAP-MSCHAPv2 — certificat IRIS-Root-CA

4. DC-IRIS-01 — Windows Server 2022

4.1 Active Directory Domain Services (AD DS)

Paramètre	Valeur
Domaine	iris.local
Niveau fonctionnel	Windows Server 2022
Contrôleur de domaine	DC-IRIS-01.iris.local — 192.168.50.10
DNS interne	192.168.50.10 — zone iris.local
Sites AD	IRIS-NICE (sous-réseau 192.168.50.0/24)

4.2 Structure Active Directory

Unité Organisationnelle (OU)	Contenu	GPO appliquée
OU=Etudiants,DC=iris,DC=local	Comptes étudiants	GPO-Etudiants (restriction accès)
OU=Professeurs,DC=iris,DC=local	Comptes professeurs	GPO-Profs (accès élargi)
OU=Admin,DC=iris,DC=local	Comptes administrateurs	GPO-Admin (droits complets)
OU=Ordinateurs,DC=iris,DC=local	Postes Windows joints au domaine	GPO-Ordinateurs (config standard)
OU=Serveurs,DC=iris,DC=local	Comptes serveurs	GPO-Serveurs (durcissement)

4.3 NPS / RADIUS — Authentification 802.1X

Paramètre	Valeur
Rôle Windows	Network Policy Server (NPS)
Port RADIUS Auth	1812/UDP
Port RADIUS Accounting	1813/UDP
Clients RADIUS enregistrés	SW2-IRIS (192.168.50.2) + AP2-IRIS (192.168.50.3)
Secret partagé	IrisRadius2026! (identique sur tous les équipements)
Méthode EAP	PEAP-MSCHAPv2
Politique ETUDIANTS	Groupe AD IRIS-Etudiants → VLAN 10 (Tunnel-Pvt-Group-ID=10)
Politique PROFS	Groupe AD IRIS-Profs → VLAN 20 (Tunnel-Pvt-Group-ID=20)
Politique ADMIN	Groupe AD IRIS-Admin → VLAN 30 (Tunnel-Pvt-Group-ID=30)
Auth fail	Refus → port bascule sur VLAN 99 Quarantaine

4.4 DHCP — Plages par VLAN

Étendue DHCP	Plage	Passerelle	DNS
VLAN 10 — Étudiants	192.168.10.100 – 192.168.10.200	192.168.10.1	192.168.50.10
VLAN 20 — Professeurs	192.168.20.100 – 192.168.20.150	192.168.20.1	192.168.50.10
VLAN 30 — Admin	192.168.30.100 – 192.168.30.120	192.168.30.1	192.168.50.10
VLAN 99 — Quarantaine	192.168.99.100 – 192.168.99.200	192.168.99.1	8.8.8.8

4.5 PKI — ADCS (Active Directory Certificate Services)

Paramètre	Valeur
Autorité de certification	IRIS-Root-CA (CA racine autonome)
Type	Standalone Root CA — stockée sur DC-IRIS-01
Algorithme	RSA 2048 bits — SHA-256
Durée validité CA	10 ans
Certificats émis	DC-IRIS-01 (NPS/RADIUS) — machines domaine (GPO auto-enrôlement)
Distribution CRL	http://dc-iris-01.iris.local/CertEnroll/
Utilisation	PEAP-MSCHAPv2 : clients vérifient certificat NPS via IRIS-Root-CA

4.6 GPO et FGPP

Objet	Paramètres clés
GPO-Securite-Mdp	Longueur min 12 — Complexité activée — Historique 24 — Verrouillage 5 tentatives
GPO-Certificats	Distribution automatique IRIS-Root-CA via Autorités de certification racines de confiance
GPO-Wifi	Profil 802.1X PEAP automatiquement appliqué aux postes du domaine
FGPP — Admins	PSO priorité 10 — Longueur 16 — 3 tentatives — Verrouillage 30 min
FGPP — Service	PSO priorité 20 — Longueur 24 — Sans expiration — 1 tentative

5. SRV-LINUX-IRIS — Ubuntu 22.04 + Docker

Service	Conteneur	Port	URL	Rôle
Nextcloud	nextcloud	8091/TCP	http://192.168.50.20:8091	Partage de fichiers
GLPI	glpi	8090/TCP	http://192.168.50.20:8090	Gestion de parc ITSM
OpenLDAP	openldap	389/TCP	ldap://192.168.50.20:389	Annuaire centralisé
phpLDAPadmin	phpldapadmin	8092/TCP	http://192.168.50.20:8092	Interface admin LDAP
Portainer	portainer	9443/TCP	https://192.168.50.20:9443	Admin Docker
Prometheus	prometheus	9090/TCP	http://192.168.50.20:9090	Collecte métriques

Grafana	grafana	3000/TCP	http://192.168.50.20:3000	Dashboards supervision
Alertmanager	alertmanager	9093/TCP	http://192.168.50.20:9093	Gestion des alertes

6. Sécurité réseau

Mécanisme	Implémentation	Objectif
Segmentation VLAN	6 VLANs isolés — trunks Cisco 802.1Q	Cloisonnement des flux par profil
Authentification 802.1X	NPS/RADIUS — PEAP-MSCHAPv2 sur SW2 et AP2	Accès réseau uniquement aux comptes AD valides
Quarantaine	VLAN 99 — AUTH-FAIL-VLAN sur SW2-IRIS	Isolation automatique des postes non conformes
ACL routeur	DENY VLAN99 vers VLANs internes — RT2-IRIS	Empêche la quarantaine d'accéder aux ressources
Chiffrement WiFi	WPA2-Enterprise AES/CCMP — IEEE 802.11i	Chiffrement trafic sans-fil
PKI interne	ADCS — IRIS-Root-CA — auto-enrôlement GPO	Confiance certificats PEAP
SSH durcissement	SSHv2 — timeout 60s — retries 3 sur RT2 et SW2	Accès administration sécurisé
FGPP	Politique de mots de passe renforcée par groupe AD	Comptes admins protégés renforcés

7. Supervision — Prometheus + Grafana

Composant	URL	Rôle
Prometheus	http://192.168.50.20:9090	Collecte métriques — 3 targets (DC-IRIS-01, SRV-LINUX)
Grafana	http://192.168.50.20:3000	Dashboards : Infra / AD / Docker / Réseau
Alertmanager	http://192.168.50.20:9093	Alertes email/webhook — règles CPU/RAM/disque
Node Exporter	Port 9100 sur chaque serveur	Métriques OS : CPU, RAM, disque, réseau
Windows Exporter	Port 9182 sur DC-IRIS-01	Métriques Windows Server

8. Tests de validation

Réf.	Test	Résultat attendu	Résultat obtenu	Statut
T-01	Ping RT2-IRIS depuis VLAN 50	Réponse < 1ms	0ms — 0% perte	PASS
T-02	Authentification 802.1X étudiants	VLAN 10 assigné par RADIUS	Tunnel-PVTGROUPID=10	PASS
T-03	Authentification 802.1X professeurs	VLAN 20 assigné par RADIUS	Tunnel-PVTGROUPID=20	PASS

T-04	Échec auth → quarantaine	Port bascule VLAN 99	VLAN 99 assigné automatiquement	PASS
T-05	WiFi WPA2-Enterprise étudiants	Connexion SSID IRIS-ETUDIANTS — VLAN 10	Associé — IP 192.168.10.x	PASS
T-06	DHCP VLAN 10	IP dans 192.168.10.100-200	IP attribuée — DC-IRIS-01	PASS
T-07	Résolution DNS iris.local	A 192.168.50.10	DC-IRIS-01 répond	PASS
T-08	Authentification AD domaine	Ouverture session Windows	Connexion OK — GPO appliquées	PASS
T-09	Accès Nextcloud	HTTP 200 depuis VLAN 30	HTTP 200 — page login	PASS
T-10	Accès GLPI	HTTP 200 depuis VLAN 30	HTTP 200 — page login	PASS
T-11	Prometheus cibles actives	3/3 UP	3/3 State: up	PASS
T-12	Dashboard Grafana	Métriques affichées	Dashboards Infra OK	PASS

9. Budget

Poste	**Coût HT**
Cisco ISR 1941W (RT2-IRIS)	3 200 EUR
Cisco Catalyst 2960-S (SW2-IRIS)	2 800 EUR
Cisco C9105AXI-E (AP2-IRIS)	1 400 EUR
Serveur DC-IRIS-01 (Windows Server 2022 + licences CAL)	8 500 EUR
Serveur SRV-LINUX-IRIS (Ubuntu + Docker — open source)	4 200 EUR
Infrastructure réseau (câblage, baie, onduleur)	3 300 EUR
Ingénierie et déploiement (équipe 3 pers. × 15 jours)	5 000 EUR
Total consommé	28 400 EUR
Budget alloué	50 000 EUR
Reste disponible	21 600 EUR

10. Normes et référentiels appliqués

Norme / RFC	**Application dans le projet**
IEEE 802.1X	Authentification port-based — SW2-IRIS + AP2-IRIS
IEEE 802.11i (WPA2)	Chiffrement WiFi — AES/CCMP — WPA2-Enterprise
RFC 2865	RADIUS Authentication — NPS ↔ SW2-IRIS / AP2-IRIS
RFC 2866	RADIUS Accounting — logs d'authentification
RFC 3580	RADIUS 802.1X — assignation dynamique VLAN
PEAP-MSCHAPv2	EAP Protected — tunnel TLS + MSCHAPv2 interne
ANSSI	Recommandations mots de passe, durcissement équipements réseau