

# Évolution et maintenance de la solution réseau Lan et Wifi de l'Ecole polytechnique

## Cahier des clauses techniques particulières (CCTP)

Consultation n°

MX25-094

## SOMMAIRE

<b>1</b>	<b>ABREVIATIONS.....</b>	<b>7</b>
<b>2</b>	<b>PREAMBULE .....</b>	<b>7</b>
2.1	PRESENTATION DE L'ÉCOLE ET D'IP PARIS .....	7
2.2	OBJET DU MARCHE.....	9
<b>3</b>	<b>DESCRIPTION DE L'INFRASTRUCTURE RESEAU .....</b>	<b>10</b>
3.1	ÉQUIPE.....	10
3.2	HISTORIQUE.....	10
3.3	EQUIPEMENTS ACTIFS .....	11
3.3.1	<i>LAN .....</i>	<i>11</i>
3.3.2	<i>WIFI.....</i>	<i>12</i>
3.4	INTERNET.....	17
3.5	ASPECTS LOGIQUES.....	17
3.6	POPULATIONS .....	18
3.6.1	<i>Connexion à l'annuaire d'entreprise .....</i>	<i>18</i>
3.7	SCHEMA GLOBAL .....	19
3.7.1	<i>Présentation des locaux techniques principaux .....</i>	<i>20</i>
3.8	SCHEMA FONCTIONNEL DE L'AUTHENTIFICATION LAN ET WIFI .....	21
3.9	SCHEMA DE LA SOLUTION D'ADMINISTRATION XIQ-SE ET DES NACS.....	22
3.10	ÉTAT DES SITES.....	23
3.11	LISTE DES SERVEURS DU RESEAU EXTREME .....	24
3.12	ADMINISTRATION DES EQUIPEMENTS.....	24
3.13	LE PORTAIL ARTEMIX D'AUTHENTIFICATION 802.1X ET MAB .....	25
<b>4</b>	<b>DESCRIPTION DES PRESTATIONS A REALISER.....</b>	<b>25</b>
4.1	POSTE 1 : PRESTATION FORFAITAIRE .....	26
4.2	POSTE 2 : PRESTATIONS A BON DE COMMANDE .....	32
4.2.1	<i>Maintenance materielle et logicielle du parc.....</i>	<i>32</i>
4.2.2	<i>SOLUTION LOAD BALANCER.....</i>	<i>33</i>
4.2.3	<i>unité d'œuvres .....</i>	<i>34</i>
4.2.4	<i>accessoires et licences.....</i>	<i>34</i>
<b>5</b>	<b>TABLES DES FIGURES .....</b>	<b>35</b>

5.1	ANNEXES .....	36
	ANNEXE 1 .....	36
	ANNEXE 2 : .....	36
	ANNEXE 3 : .....	36
	ANNEXE 4 : .....	36
	ANNEXE 5 : .....	36
	ANNEXE 6 : .....	36
	ANNEXE 7 : .....	36

## 1 ABREVIATIONS

- Une liaison 1 Gigabits/Seconde sera écrite 1G.
- Une liaison 10 Gigabits/Seconde sera écrite 10G.
- Un To correspond à un Téra Octets de données.
- 100M : une liaison au débit de 100 Mégabits/seconde.
- ACL(s) : Access-list (règle de filtrage).
- SD : Service Desk, le Centre d'Assistance de la Direction des Systèmes d'Information de l'Ecole polytechnique (helpdesk de 6 personnes).
- LT : un Local Technique, où se situent des équipements réseaux et le câblage des prises utilisateurs.
- SI : Système d'information

## 2 PREAMBULE

### 2.1 PRESENTATION DE L'ÉCOLE ET D'IP PARIS

L'École polytechnique a pour mission de former des hommes et des femmes capables de concevoir et de mener des activités complexes et innovantes au plus haut niveau mondial, en s'appuyant sur une culture à dominante scientifique d'une étendue, d'une profondeur et d'un niveau exceptionnels, ainsi que sur une forte capacité de travail et d'animation.

Fidèle à son histoire et à sa tradition, l'École forme de futurs responsables de haut niveau, à forte culture scientifique, voués à jouer un rôle moteur dans le progrès de la société par leurs fonctions dans les entreprises, les services de l'État et la recherche.

Son projet pédagogique est de former des hommes et des femmes de caractère, équilibrés, aptes au travail en équipe, associant à la rigueur l'écoute des autres et la liberté d'esprit, dotés d'une capacité exceptionnelle d'analyse et de synthèse, et capables d'analyser, de concevoir, de construire et de mettre en œuvre des systèmes complexes.

Cette formation repose sur un programme éducatif unique, réalisant un équilibre entre :

- Un enseignement scientifique, pluridisciplinaire, de très haut niveau ;
- Une ouverture vers des disciplines littéraires et artistiques et la pratique de langues étrangères ;
- Une formation éthique, humaine et sportive.

Elle apprend aux élèves à travailler avec rigueur, dans le respect des faits et l'honnêteté intellectuelle, de maîtriser les technologies actuelles et d'anticiper celles de demain. Elle leur permet aussi d'acquérir une culture d'une richesse et d'un

niveau exceptionnel, tout en développant chez eux le travail en équipe, une ouverture aux problèmes de société et aux attentes de la collectivité, un sens aigu de la responsabilité individuelle.

Elle est mise en œuvre en associant à un corps enseignant de très haut niveau, un centre de recherche internationalement reconnu et un encadrement militaire à qui a été confié l'essentiel de la formation éthique, humaine et sportive.

Le régime de l'internat crée les conditions d'une vie associative et collective intense sur le campus et favorise l'initiative et la créativité de chacun.

Conformément aux valeurs et à la tradition qui sont les siennes, depuis plus de 200 ans, l'École est accessible à tous sans distinction d'origine ou de condition sociale. Le seul critère d'admission est la sélection par concours des étudiants les plus aptes à se réaliser dans ce projet.

Pour former des polytechniciens ouverts sur le monde et capables d'exceller dans des environnements multiculturels et multinationaux, l'École accueille un fort contingent d'élèves étrangers et intègre dans son cursus des stages et des formations longues hors de France.

En associant à son cœur historique de formation, le cycle polytechnicien d'ingénieur, des formations aux normes internationales, bachelor, masters et thèses, elle se positionne dans l'offre mondiale et valorise sa spécificité.

Sous la responsabilité du président du Conseil d'Administration, l'École s'articule autour de trois ensembles, les "élèves et enseignants" (3800 personnes dont 1650 élèves polytechniciens, DF<sup>1</sup>), la "recherche" (2300 personnes dont 400 élèves masters ou doctorants réparties dans 22 Unités Mixtes de Recherche (UMR), DAER<sup>2</sup>) et "la direction générale et l'administration" (1700 personnes, **D**irection **G**énérale, **S**ecrétariat **G**énéral) et sur les directions fonctionnelles suivantes : la **D**irection de la **F**ormation **H**umaine et **M**ilitaire (DFHM), la **D**irection des **R**elations **E**xérieures (DRE), la **D**irection du **C**abinet (DCAB), la **D**irection du **C**oncours (DCA), la **D**irection des **S**ystèmes d'**I**nformation (DSI).

Le centre de recherche de l'École (23 laboratoires) représente au niveau informatique un ensemble virtuellement cloisonné des autres populations. Il est soumis aux dispositions de l'arrêté du 3 juillet 2012<sup>3</sup> concernant la protection du patrimoine scientifique et technique de la nation.

Le campus de l'École polytechnique s'étend sur une superficie de 180 Ha et comprend environ 100 bâtiments. Les bâtiments principaux se répartissent le long d'une diagonale de 1.200 mètres de long.

Tous les personnels disposent d'un poste téléphonique IP ou d'un softphone, ainsi que d'un poste de travail informatique, relié via le réseau local de l'École à Internet.

L'Institut Polytechnique de Paris est un établissement public d'enseignement supérieur et de recherche qui réunit six Grandes Écoles d'ingénieurs françaises : l'École polytechnique, l'ENSTA Paris, l'ENSAE Paris, Télécom Paris, Télécom SudParis et ENPC. Sous l'égide de l'Institut, elles mettent en commun leur expertise bicentenaire afin de poursuivre deux grandes ambitions : développer des programmes de formation d'excellence et une recherche de pointe. Grâce à l'ancrage de ses cinq Écoles fondatrices, l'Institut Polytechnique de Paris se positionne comme une institution d'enseignement et de recherche leader en France et à l'international. En effet, l'École polytechnique, l'ENSTA Paris, l'ENSAE Paris, Télécom Paris et Télécom SudParis ont contribué aux révolutions industrielles et technologiques majeures de ces deux derniers siècles. Parmi les diplômés de ces Écoles figurent plusieurs prix Nobel, ainsi que de grandes personnalités du monde politique, économique et de la recherche.

---

<sup>1</sup> **D**irection des **F**ormations

<sup>2</sup> **D**irection **A**djointe de l'**E**nseignement et la **R**echerche

<sup>3</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026140136&dateTexte=&categorieLien=id>

L'Institut Polytechnique de Paris développe des programmes de formation et de recherche pluridisciplinaires, s'appuyant sur une communauté de 1000 enseignants-chercheurs oeuvrant au sein de dix départements disciplinaires. Cette approche croisée crée des synergies inédites entre différents domaines, favorisant par exemple l'application des nouvelles technologies aux domaines d'ingénierie traditionnels tels que la physique ou les transports. Le transfert de connaissances vers l'économie et la société est au coeur des missions de l'Institut, dont le réseau d'incubateurs et l'écosystème dynamique favorise l'innovation de pointe et stimule l'inventivité des étudiants

Depuis 2015, LA FIBRE ENTREPRENEUR est le **premier centre intégré en faveur de l'entrepreneuriat et de l'innovation à l'École polytechnique**. Cet espace d'une surface totale de 2 500m<sup>2</sup> constitue un espace unique de création, d'expérimentation et de prototypage, d'enseignement, d'incubation et d'accélération, et d'échange avec les investisseurs. Conçu selon le concept des accélérateurs les plus modernes au monde, il fonctionne en étroite interaction avec des incubateurs partenaires (Télécom ParisTech, HEC...) et avec les institutions de valorisation présentes sur le campus de Paris-Saclay.

## 2.2 OBJET DU MARCHÉ

Le présent marché a pour objet l'évolution et la maintenance de la solution réseau Lan et Wifi de l'Ecole polytechnique. L'évolution doit permettre d'avoir la plus grande performance sur le maintien en conditions opérationnelles du parc existant en respectant les plus hauts standards de sécurité des SI. Les évolutions (dont les extensions matérielles) et la maintenance concernent le parc réseau Lan et Wifi existant du constructeur EXTREME NETWORKS qui représente la majorité du marché décrit ci-après.

La DSI n'étant pas organisée pour les astreintes, l'architecture et ses évolutions doivent répondre aux besoins de robustesse, de résilience et d'efficacité sur le maintien en conditions opérationnelles du parc existant et de ses évolutions.

Le marché public est découpé en 2 postes :

- Poste 1 – Prestation forfaitaire :
  - Évolution de la plate-forme d'administration réseau XIQ-SE, CloudIQ, automatisation, remplacement de commutateurs et évolution de la solution Wifi et du portail captif wifi.
- Poste 2 – Prestations à bons de commande :
  - Maintenance matérielle et logicielle du parc
  - Solution load balancer
  - Unités d'œuvre d'ingénierie pour réaliser des prestations complémentaires sur la durée de vie du marché
  - Accessoires et licences liés aux matériels réseaux et Wifi de l'Ecole avec leurs coûts de maintenance

NOTA : le titulaire du présent marché est réputé détenir toutes les informations nécessaires à la réalisation de la prestation à la date de notification, et ne peut se prévaloir d'aucune absence d'information pour justifier d'éventuels délais dans l'accomplissement de sa mission.

### 3 DESCRIPTION DE L'INFRASTRUCTURE RESEAU

#### 3.1 ÉQUIPE

Six ingénieurs réseaux, sous la responsabilité du Responsable des télécommunications, ont actuellement en charge le maintien à niveau opérationnel de l'infrastructure réseau (Data, Wi-Fi et ToIP), ainsi que son évolution.

#### 3.2 HISTORIQUE

En 2016, l'École a remplacé ses 2 cœurs de réseaux par des Extreme Networks Black Diamond 8810, permettant ainsi de disposer d'un nombre important de ports 10G et de répondre aux besoins constants de l'augmentation de la bande passante.

En 2017, l'École a procédé à la mise à jour majeure de sa solution de téléphonie sur IP Avaya Communication Manager en version 7.

En 2020, l'École a remplacé ses deux pares-feux par des Palo Alto 5250, permettant ainsi de disposer de 16 ports 10G, de 4 ports 40G QSFP+/100G QSFP28, afin de répondre aux besoins constants de l'augmentation de la bande passante.

En 2021, l'École a procédé à la mise à jour majeure de sa solution de téléphonie sur IP Avaya Communication Manager en version 8.

En 2023, l'École a remplacé ses 2 cœurs de réseaux par des VSP 7400 d'EXTREME NETWORKS (technologie Fabric).

En 2024, l'École a procédé à la mise à jour majeure de sa solution de téléphonie sur IP Avaya Communication Manager en version 10. L'usage de téléphones physiques tend à disparaître au profit de la solution de softphonie Avaya Workplace.

### 3.3 EQUIPEMENTS ACTIFS

Les divers backbones s'insèrent dans l'infrastructure redondée du réseau de données selon le schéma ci-dessous.

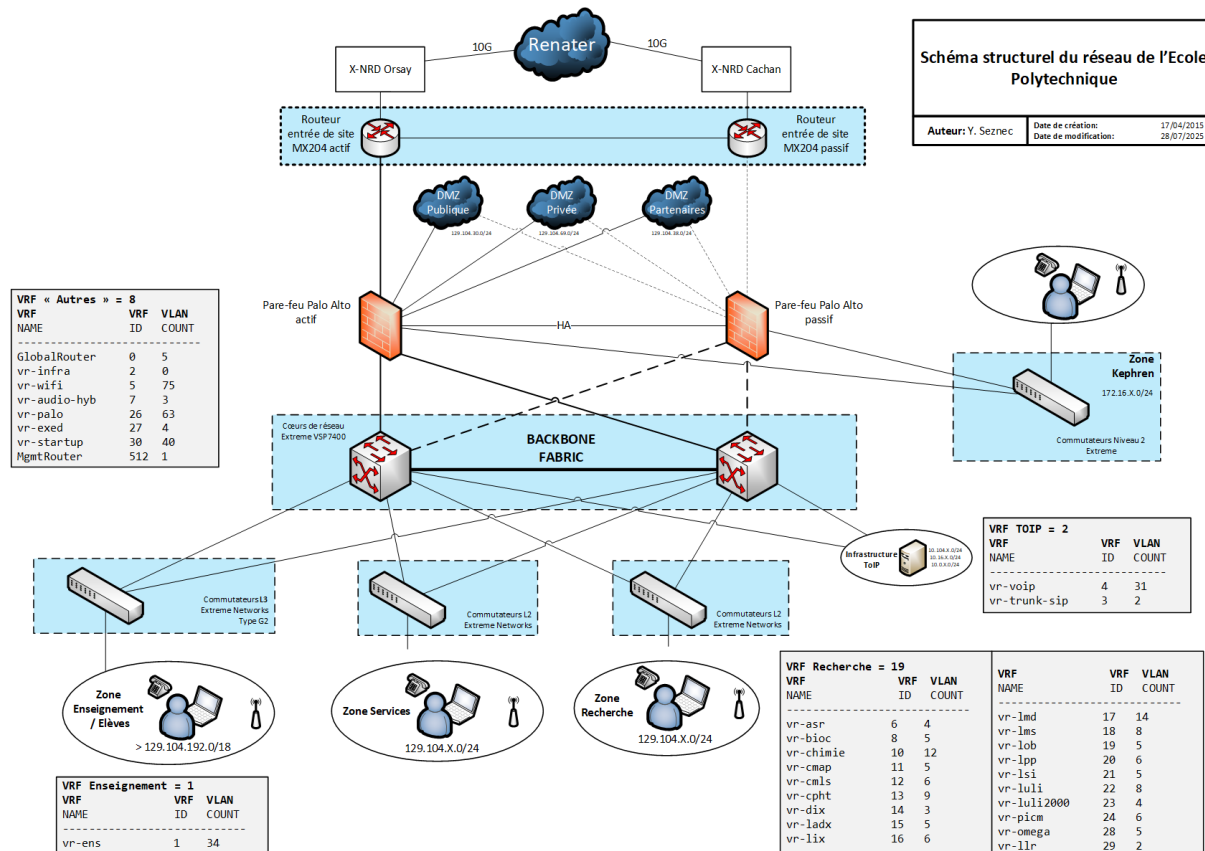


Figure 1: Schéma structurel du réseau de l'Ecole Polytechnique

#### 3.3.1 LAN

Le backbone du réseau de polytechnique peut être divisé en trois catégories d'équipements de routage :

- Backbone du réseau Enseignement/Recherche : des commutateurs et routeurs Extreme Networks VSP7400 (de niveau 3) pour les « coeur de réseaux » afin de raccorder les bâtiments, des switches 5420 pour les pieds de bâtiments (Technologie Fabric) ainsi que des X460-G2 de niveau 3 (routage statique) pour les logements des élèves
- Backbone du réseau "Administration" : 1 cluster de pare-feu Palo-Alto PA5250 (de niveau 3)
- Backbone ToIP : 2 commutateurs Extreme Networks de type X460-G2 (de niveau 3)

Les équipements de distribution sont divisés suivant plusieurs générations d'équipements :

- De type Legacy : X250, X450 (en cours de remplacement par de l'Universal Hardware)
- De type G1 : X430, X440, X460, X590, X670 (en cours de remplacement par de l'Universal Hardware)
- De type G2 : X440G2, X460G2 (-mp), X620
- De type G3 : X435, X465
- De type VPEX (V400)
- Universal Hardware : 4220, 5320, 5420

Les équipements de périphérie sont composés de commutateurs PoE et/ou PoE+, 24 ou 48 ports principalement, et empilables (jusqu'à 8 commutateurs) afin de permettre le raccordement de téléphones, bornes Wi-Fi et caméras. La quasi-totalité des équipements de périphérie est double-attachée en MLAG sur 2 peers de la Fabric (sur un total de 3 actuellement).

### 3.3.2 WIFI

L'infrastructure existante est décrite ci-après :

2 ESX Dell R440 hébergeant tous les serveurs virtuels Wifi dont :

- 2 contrôleurs Wi-Fi Wing (VX9000) de l'École polytechnique et ses bornes associées,
- de la solution CloudIQ Wireless et ses bornes associées,
- de la solution Ucopia hébergeant le portail captif Wi-Fi pour les visiteurs et le BYOD (dont les comptes sont stockés localement),
- 2 contrôleurs physiques NX7510 assurant la fonction de segmentation pour le portail captif « invités »,
- La licence VMware associée aux ESX essentials VMware 7 6 CPU (contrat n°477913657)
- La licence Veeam pour les sauvegardes, contrat n°02344869 en mode basique (4 sockets, support ID 03734897).

Les détails matériels et logiciels sont fournis dans les tableaux ci-après :

	Modèle du serveur	CPU	Nombre de socket	RAM	Stockage	Version ESXi	Numéro de série
ESXi 1	Dell PowerEdge R440	Intel Xeon Gold 6130 @ 2.10GHz	2	256 GB (8x32GB)	RAID5 4.36TO (5+1 x 1.2Tb SAS ST1200M M0099)  RAID1 1.75To (2x Intel 1.92Tb SSDSC2K G019T7R)	6.7U3	DLYNNR2
ESXi 2	Dell PowerEdge R440	Intel Xeon Gold 6130 @ 2.10GHz	2	256 GB (8x32GB)	RAID5 4.36TO (5+1 x 1.2Tb SAS ST1200M M0099)  RAID1 1.75To (2x Intel 1.92Tb SSDSC2K G019T7R)	6.7U3	DLZMNR2

Les 2 appliances physiques NX7510 :

	Type de matériel	Version	Numéro de série
<b>Contrôleur NX7510 1</b>	NX-7510-100R0-WR	7.7.1.11-007R	16350021110012
<b>Contrôleur NX7510 2</b>			16365021110072

Détail des serveurs virtuels :

	Type de matériel	vCPUs	RAM	Stockage	Version	Licence	Numéro de série
<b>Ucopia 1</b>	UV2000	12	16 Go	2 To	7.2.5	Advance 5000 LR	V2404565
<b>Ucopia 2</b>		12	16 Go	2 To			V2404566
<b>Contrôleur WiNG 1</b>	VX9000	18	40 Go	500 Go	7.7.1.11-007R	560 AAP	3B53361B971D79B5
<b>Contrôleur WiNG 2</b>		18	40 G0	500 G0			18733E7ADB6F87DD

Campus (hors logements étudiants) => Infrastructure Extreme Networks WiNG

- 2 Contrôleurs physiques NX 7510
- 2 Contrôleurs VX 9000
- 2 UCOPIA (Guest et BYOD)
- 343 bornes (315 AP7632, 15 AP8432, 11 AP310, 1 AP510 ; 1 AP7612...)

Actuellement, 3 SSIDs sont en production sur l'infrastructure Wi-Fi de l'École polytechnique :

- Eduroam
- Guest
- BYOD

Il y a également 4 SSIDs (en partie cachés) diffusés dans des zones restreintes pour des besoins particuliers.

Tous ces SSID sont bridés à l'AP.

### 3.3.2.1 SSID EDUROAM

Le SSID eduroam vise à offrir un accès sans fil sécurisé à l'Internet aux personnels et aux étudiants de la communauté enseignement supérieur/recherche lors de leurs déplacements. Les utilisateurs d'un établissement membre du projet disposent alors de cet accès depuis tous les autres établissements membres, en utilisant leurs identifiants habituels.

Une authentification 802.1x liée à l'annuaire LDAP est nécessaire pour se connecter. Le client se retrouvera dans le VLAN associé à son service en fonction d'un attribut présent sur son compte utilisateur (pour les étudiants et personnels de l'Ecole polytechnique).

Le mécanisme d'authentification exploite le protocole 802.1x EAP-TTLS-PAP.

L'attribut utilisé est le suivant => X-Vlan-Wifi. Lors de la création d'un utilisateur nous associons à cet attribut le VLAN Wi-Fi de son service. Par conséquent, lors de l'authentification, le serveur RADIUS utilisé placera dynamiquement l'utilisateur dans le réseau associé à cet attribut.

Le serveur RADIUS utilisé est le NAC Extreme (Network Access Control).

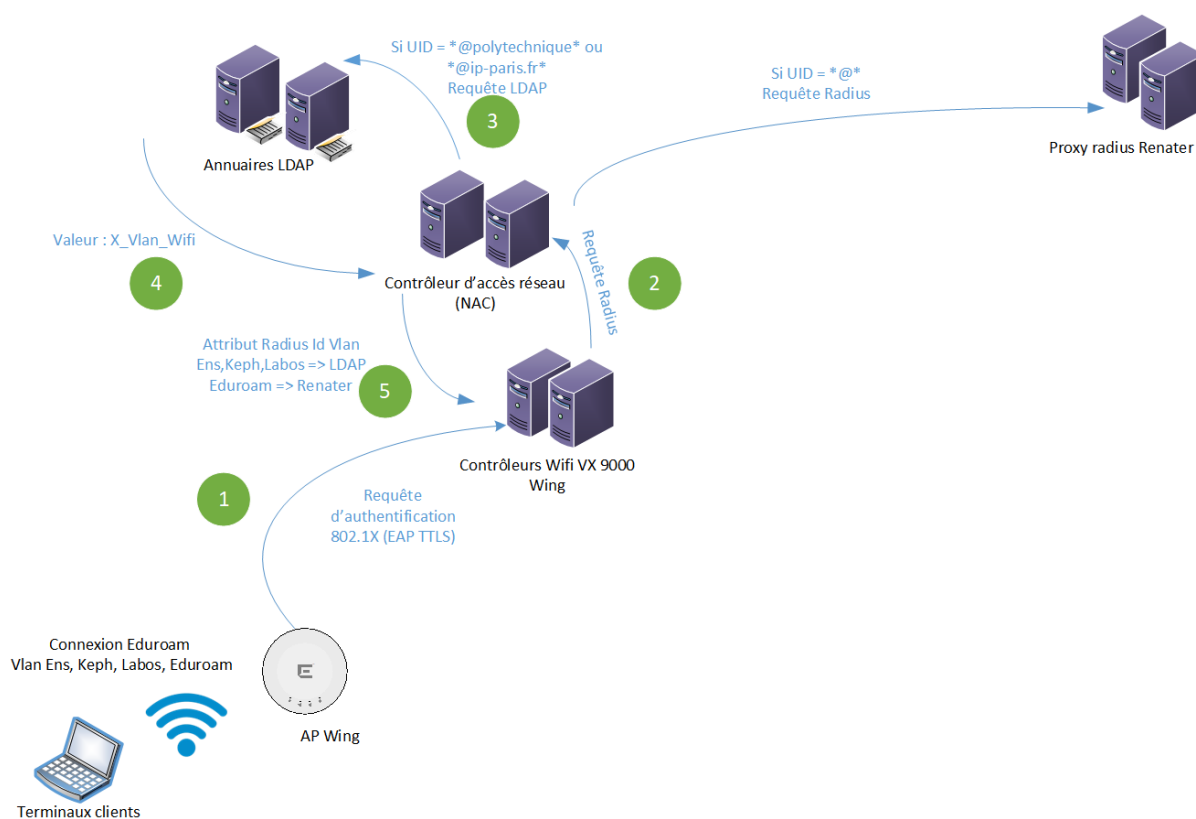


Figure 2: Schéma des flux d'authentification du SSID eduroam

### 3.3.2.2 SSID GUEST

Le SSID Guest est dédié aux visiteurs de l'École polytechnique. N'importe quel utilisateur peut se connecter à ce réseau. Une fois connecté, l'utilisateur est redirigé vers le portail captif de la solution Ucopia.

Il est nécessaire de s'enregistrer sur le portail captif pour bénéficier d'un compte valable 5 jours.

Un portail de délégation est disponible pour créer des comptes de longue durée pour des événements.

La borne Wifi monte un tunnel vers les NX7510 pour acheminer les flux utilisateurs jusqu'à l'Ucopia.

Celui-ci fournit une adresse IP au client avec comme passerelle par défaut et DNS le cluster Ucopia.

Les flux utilisateurs transitent ainsi via l'Ucopia.

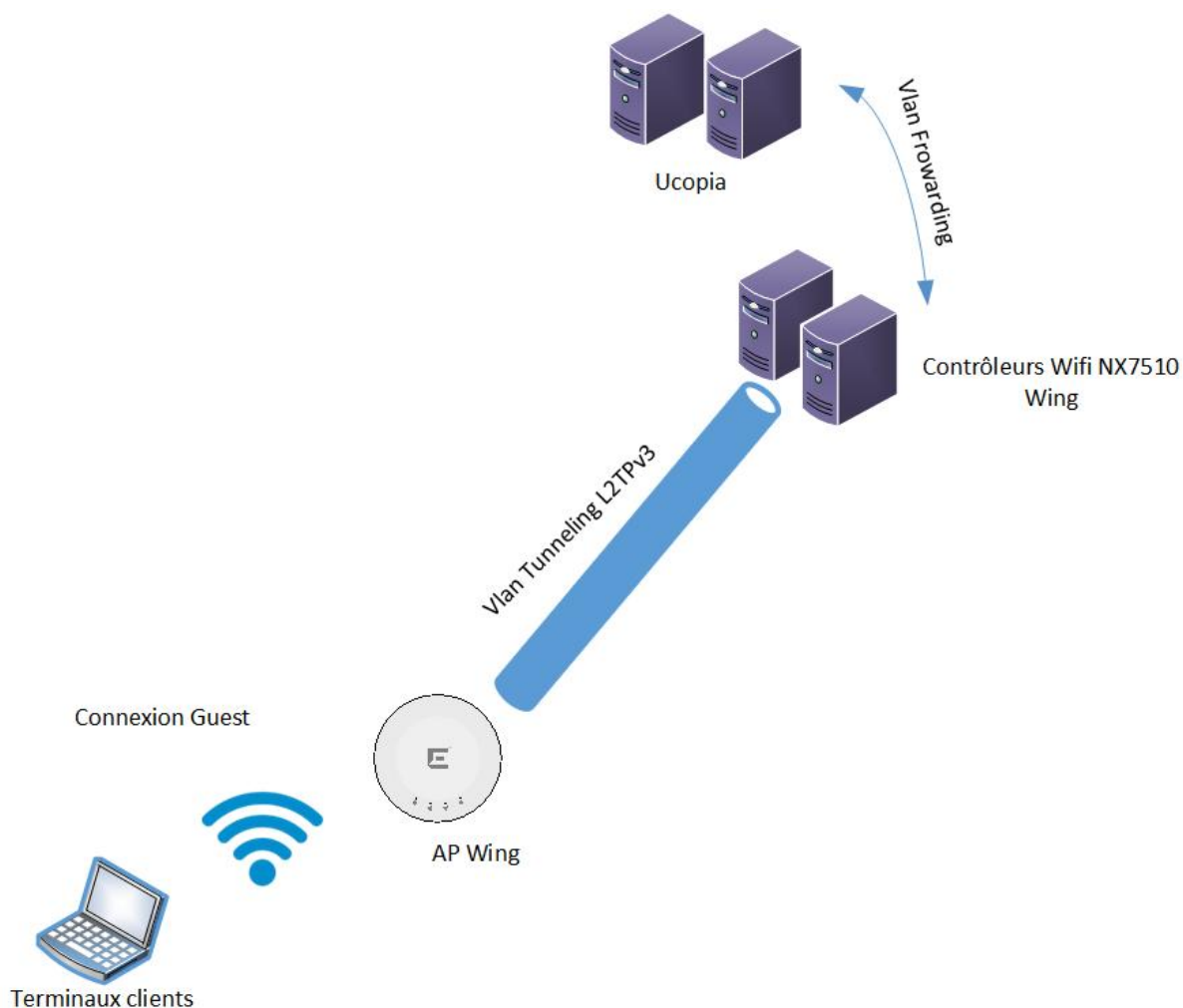


Figure 3: Schéma des flux d'authentification sur le portail captif du SSID Guest

### 3.3.2.3 SSID BYOD

Ce SSID sera arrêté à l'été 2026, il est donc mentionné à titre informatif et n'a pas à être pris en compte dans l'offre du titulaire.

Le SSID BYOD est dédié aux terminaux WiFi dont les terminaux ne sont pas compatibles avec le 802.1X.

Avant de se connecter au SSID, il est nécessaire de déclarer l'adresse MAC du terminal à connecter sur le portail captif dédié au BYOD. Ce portail captif spécifique au BYOD est aussi assuré par la solution Ucopia.

Les flux utilisateurs sont routés par l'Ucopia.

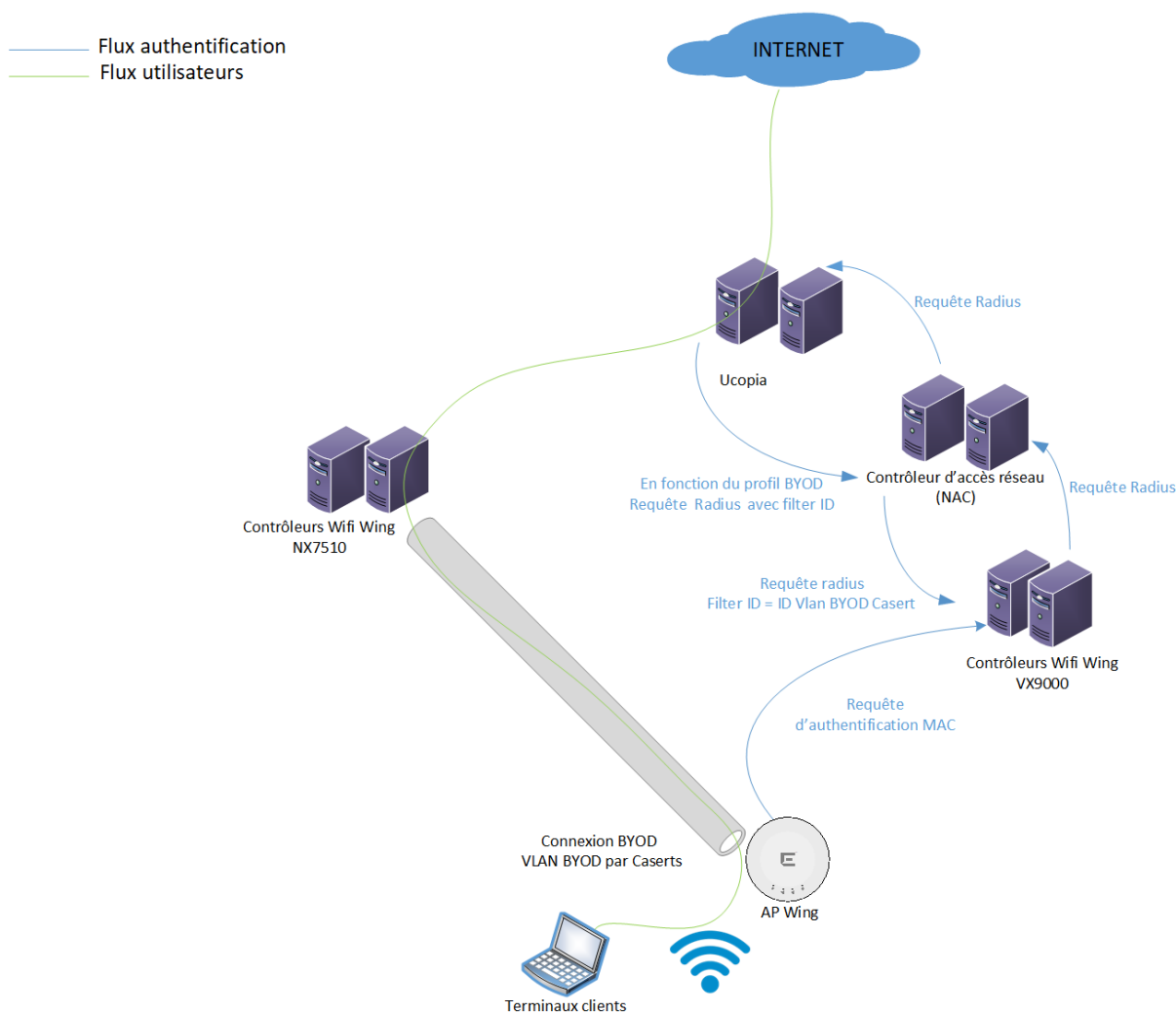


Figure 4: Schéma de flux d'authentification par adresse MAC sur le SSID BYOD

### 3.3.2.4 SCHEMA GLOBAL DES FLUX D'AUTHENTIFICATION DES UTILISATEURS EN WIFI

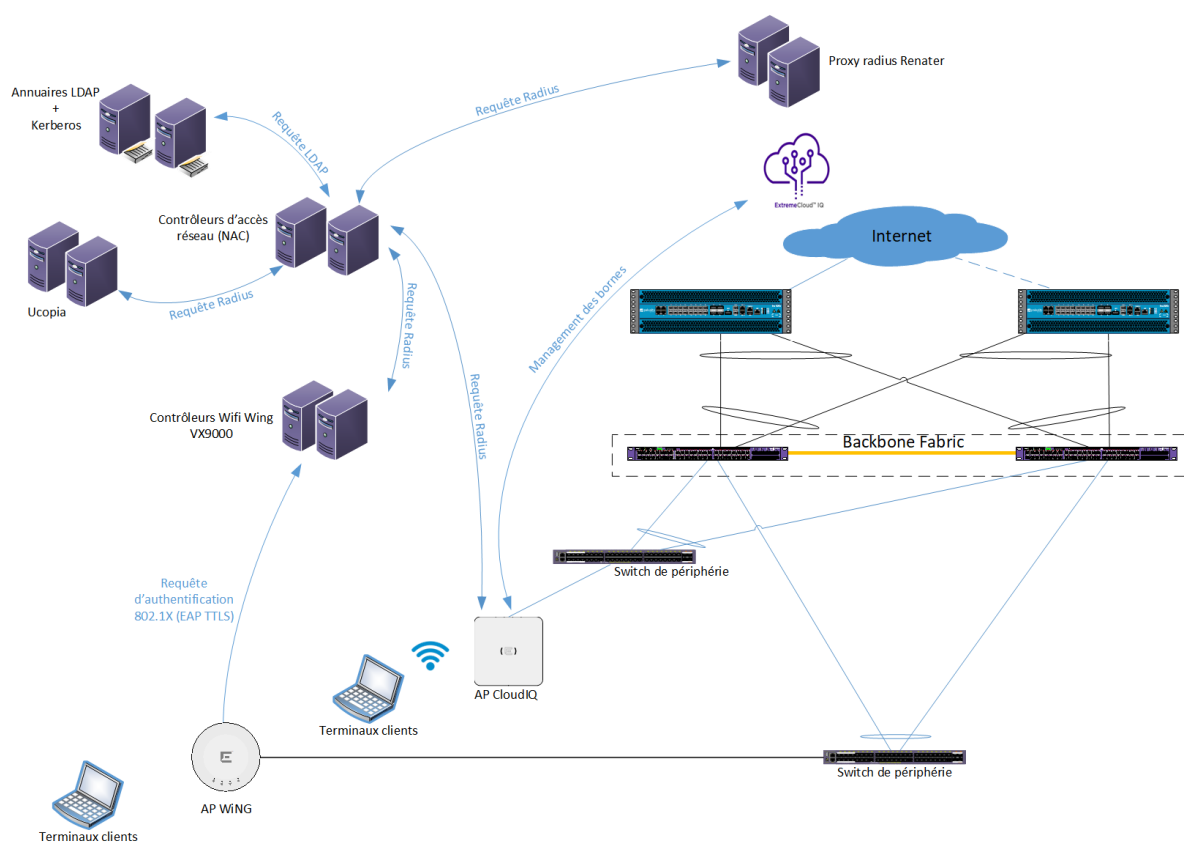


Figure 5: Schéma global des flux d'authentification WiFi WiNG et CloudIQ

## 3.4 INTERNET

Notre accès internet est connecté au réseau national de la recherche (RENATER) par deux liens 10G nominal/secours via le Réseau Haut Débit de l'Université Paris-Saclay et par 2 liens 1G via SFR qui nous garantissent une haute disponibilité (Multihoming BGP).

## 3.5 ASPECTS LOGIQUES

Dans leur très grande majorité, les flux sont composés d'une part de flux intra-groupe et d'autre part de flux vers l'internet. Les flux intergroupes sont très faibles. Ceci est vrai y compris pour les trafics de sauvegardes qui demeurent confinés à une même matrice de commutation.

En matière d'adressage IP, l'École possède la classe B 129.104.0.0/16 qu'elle subdivise en 254 sous-réseaux et dispose aussi du préfixe IPv6 2001:660:3026::/64.

La gestion des plages IP est assurée par la DSI. Les réseaux des services et des laboratoires utilisent la plage 129.104.0.0 à 129.104.125.0. Les adresses IP sont gérées en statique dans le DNS de l'X.

Le réseau administratif utilise la plage 172.16.128.0 à 172.16.191.0, translatée par le pare-feu Palo Alto PA5250 en 129.104.128.0 à 129.104.191.0. Les adresses IP sont délivrées par des serveurs DHCP Windows redondés.

Les sous-réseaux 129.104.192.0 à 129.104.254.0 sont utilisés pour l'enseignement et les réseaux élèves. A l'exception des salles de cours, les adresses IP des réseaux « élèves » sont dynamiques grâce au 802.1x utilisé dans ces sous-réseaux.

Le réseau de la téléphonie sur IP (ToIP) utilise la plage 10.0.0.0 à 10.104.255.255.

Les cœurs de réseaux VSP contiennent 379 VLANs répartis en 32 routeurs virtuels (VRF). 245 VLANs sont routés par notre cluster de pare-feux.

## 3.6 POPULATIONS

Les personnels ainsi que les étudiants et visiteurs ont également la possibilité de se connecter au Wi-Fi. Ils disposent pour cela de plus de 1500 bornes réparties sur le campus (salles de cours, amphithéâtres, logements étudiants, bureaux...). Afin de couvrir l'ensemble des utilisateurs, nous comptons deux équipements minimums par usager.

Trois principales catégories de postes de travail sont mises en œuvre : PC Windows, MAC OS et Linux.

---

### 3.6.1 CONNEXION A L'ANNUAIRE D'ENTREPRISE

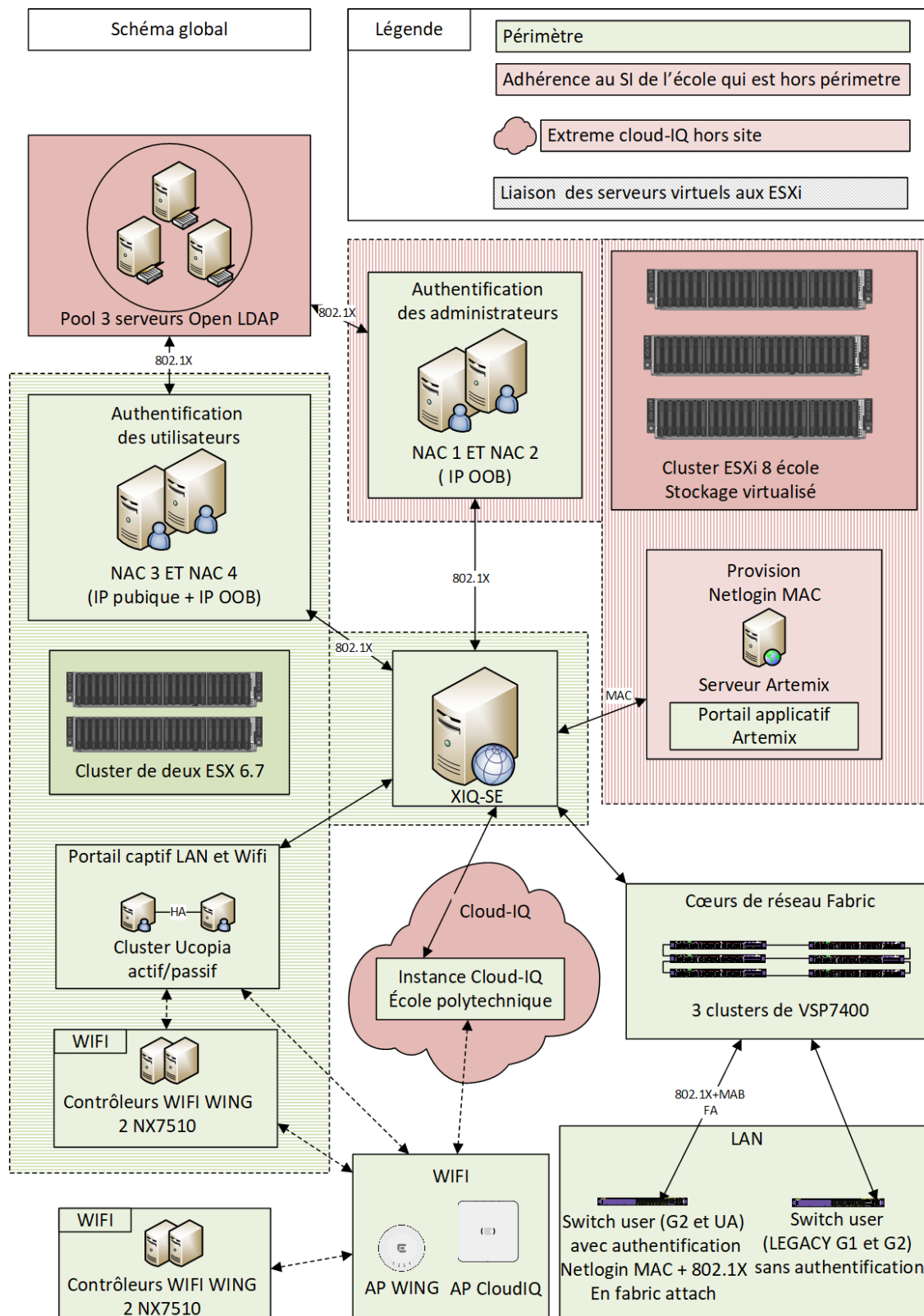
Tous les utilisateurs de l'Ecole sont renseignés dans l'annuaire LDAP de l'École polytechnique.

Toutes les informations techniques ainsi qu'un exemple de fiche annuaire sont disponibles dans l'[annexe 1](#)

L'ensemble des services proposés par le titulaire doit respecter la connexion à l'annuaire d'entreprise.

### 3.7 SCHEMA GLOBAL

Le schéma ci-dessous présente la situation de toutes les briques et leurs interactions.



### 3.7.1 PRESENTATION DES LOCAUX TECHNIQUES PRINCIPAUX

Les hyperviseurs et serveurs sont répartis sur trois locaux techniques principaux (LTP) ci-dessous :

- 0-0-0, local technique principal du bâtiment zéro
- 7-1-0, local technique principal du bâtiment 7
- 20-0-0, local technique principal du bâtiment 20

Les cœurs de réseaux sont composés de 3 clusters de VSP74000 répartis sur les locaux ci-dessous :

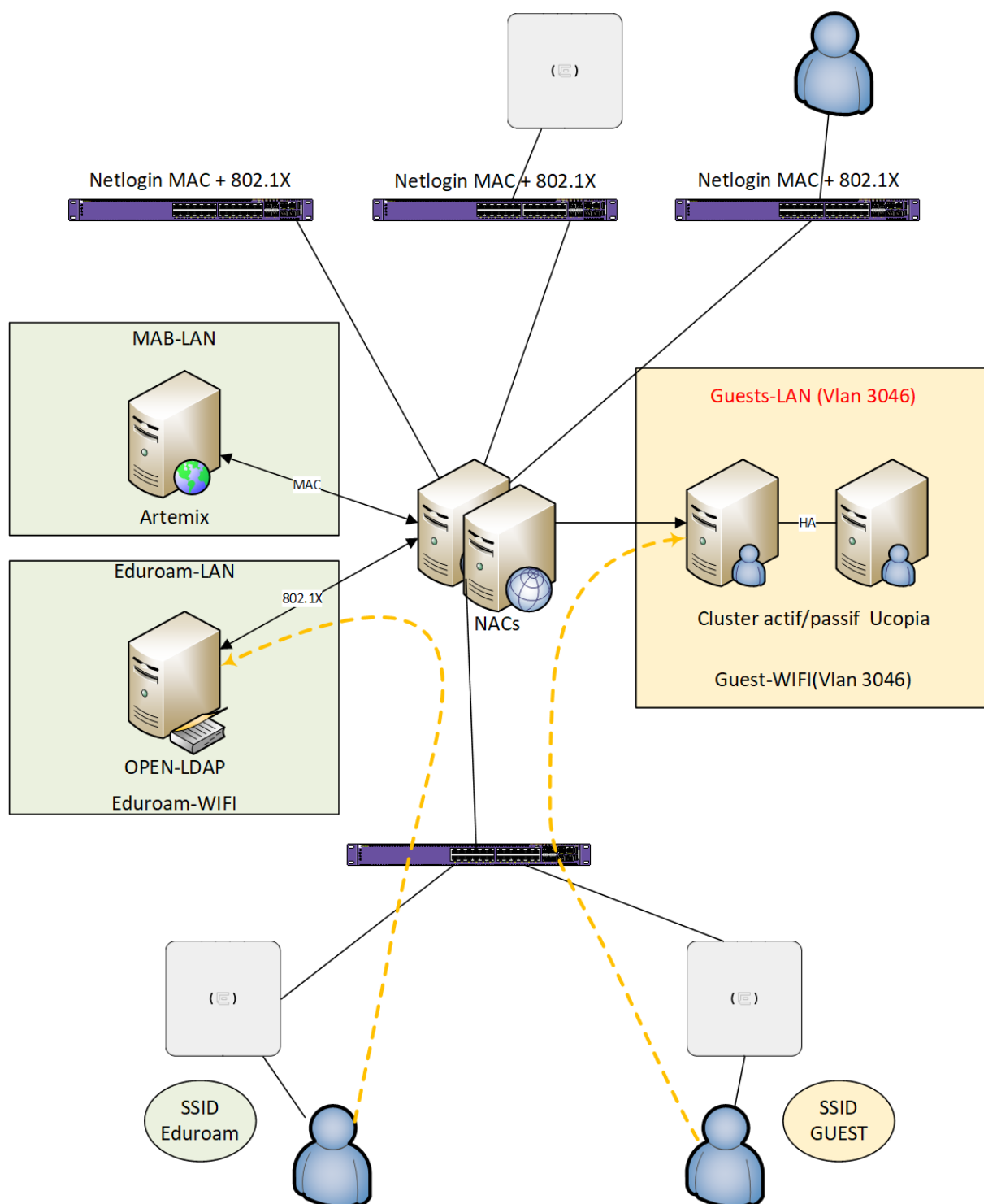
- 7-1-0, local technique principal du bâtiment 7
- 5-0-6, local technique principal du bâtiment 5

L'ensemble des raccordements entre les locaux techniques sont fournis en fibre optique monomode en connectique LC.



Figure 6. Localisation sur le campus polytechnique des quatre LTP

### 3.8 SCHEMA FONCTIONNEL DE L'AUTHENTIFICATION LAN ET WIFI



Les utilisateurs et les bornes s'authentifient sur les switches Extreme à partir de la gamme G2.  
 Les administrateurs réseaux s'authentifient sur l'interface OOB des switches Extreme.  
 Les utilisateurs du WiFi eduroam s'authentifient sur les bornes WiFi.

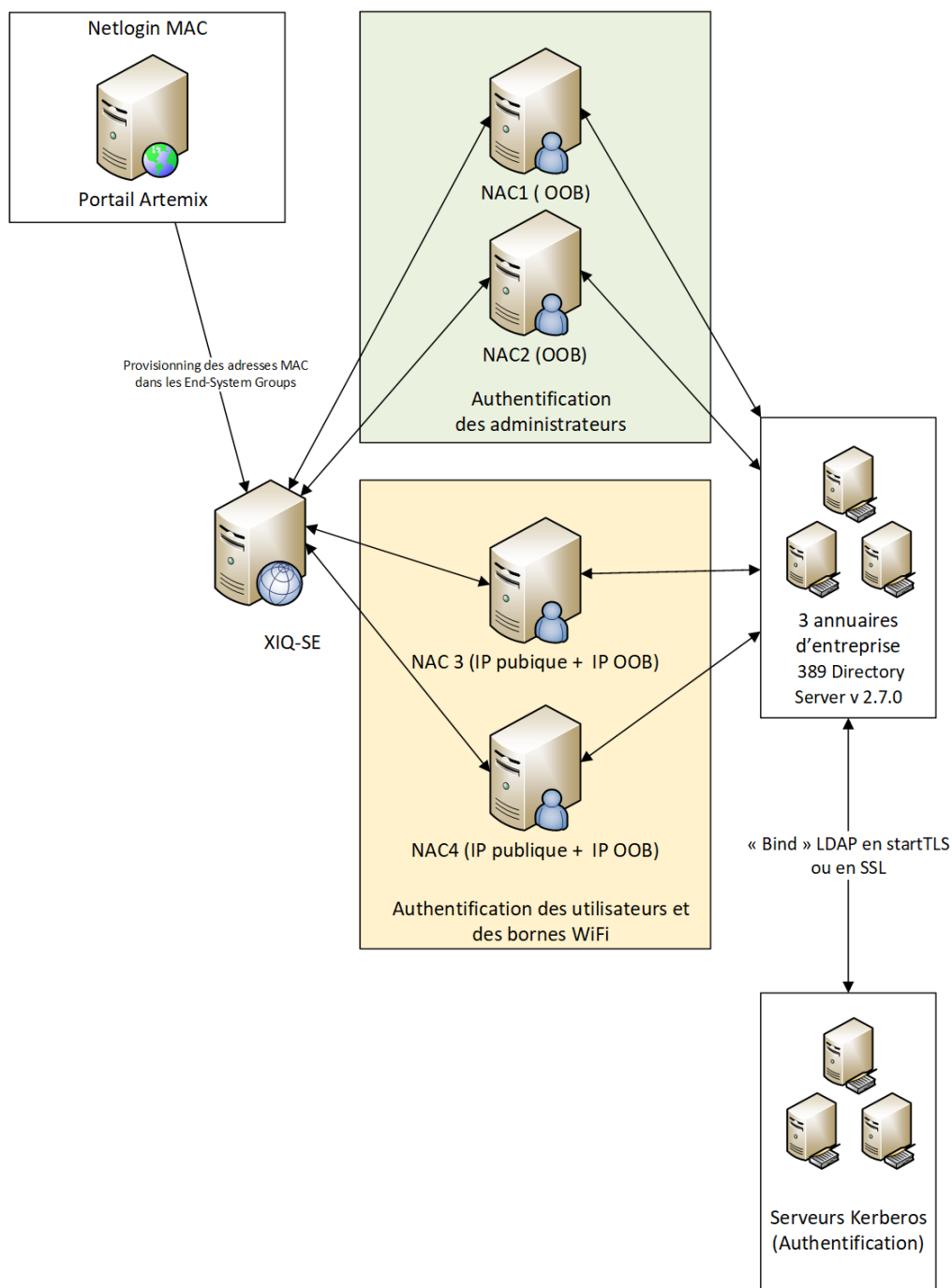
Sur les serveurs d'authentification NAC nous déclarons en tant que NAS-IP l'ensemble des switches et bornes WiFi CloudIQ.

Les switches de gamme G2 et supérieures contactent les NACs pour l'authentification des utilisateurs filaires et les bornes WiFi.

Les bornes WiFi contactent les NACs pour l'authentification des utilisateurs WiFi du SSID eduroam.

Les NACs renvoient les requêtes d'authentification vers les serveurs OpenLDAP qui interrogent des serveurs Kerberos où sont stockés les mots de passe.

### 3.9 SCHEMA DE LA SOLUTION D'ADMINISTRATION XIQ-SE ET DES NACS



Le service XIQ-SE est hébergé sur 1 serveur virtualisé et déployé sur l'infrastructure de virtualisation composée de deux hyperviseurs ESXi en version 6.7. La licence essentiel ne permet pas le HA des VM. Il n'y a pas de Vcenter sur ce cluster d'ESXi.

L'architecture actuelle d'authentification autour du serveur on premise XIQ-SE est la suivante :

- 4 serveurs NACs non équivalents
  - 2 serveurs NACs pour le Radius Management-Access (VR-MGMT).
  - 2 serveurs NACs pour le Radius Netlogin (VR-Default).
- 3 serveurs d'annuaire d'entreprise Open LDAP + 3 serveurs Kerberos
- 1 portail qui permet le provisionnement d'adresses MAC via API (nommé ArtemiX et développé en Symfony).

### 3.10 ÉTAT DES SITES

Afin d'exploiter au mieux le parc de 1000 commutateurs, le pôle réseau fait évoluer ses procédures de renouvellement de matériels à l'aide de workflows sur XIQ-SE. Des workflows sont en place dans XIQ-SE pour automatiser le provisionning de nouveaux stacks par site par un onboarding temporaire. Lorsque le stack ou le switch est finalisé sans erreur dans le site temporaire d'onboarding, le stack ou switch est déplacé dans son site définitif.

L'ensemble des commutateurs réseaux est reparti sur 5 domaines ou sites différents. Chaque site/domaine possède des caractéristiques présentes dans la configuration actuelle de XIQ-SE.

Le tableau ci-dessous résume la situation actuelle :

Paramètres	MGMT	CA-CAM	GTB	LABO	KEPHREN
Mise à jour des switchs à la dernière version EXOS	X	X	X	X	X
Désactivation du VLAN par défaut (VLAN 1)	X	X	X	X	X
Désactivation de tous ports non utilisés	X	X	X	0	X
Suppression des comptes locaux	X	X	X	X	X
Activation du SSH uniquement sur l'interface MGMT OOB	X	X	X	X	X
Configuration du Nom, LT, Timezone	X	X	X	X	X
Configuration du NTP	X	X	X	X	X
Configuration du Syslog	Vr-Default	Vr-MGMT	VR-MGMT	VR-MGMT	VR-MGMT
Configuration QOS profile	0	0	0	X	X
Désactivation du EDP	X	X	X	X	X
Activation du LLDP sur tous les ports					
Configuration du s-MAC par port	1	1	5	25	2
Désactivation du ELRP	X	X	X	X	X
Activation du SLPP sur tous les ports sauf les uplink					
Configuration du DHCP Snooping sur les VLANs	X	X	X	X	X
Configuration du SNMP V3	X	X	X	X	X
Configuration du RADIUS (MGMT)	X	X	X	X	X
Configuration du Radius (Netlogin)	0	0	0	X	X
UPM	0	0	0	X	X
Vlan MGMT	862	OOB	OOB	OOB	OOB
Création des VLAN par défaut	0	d aeos d cam	Liste connue	0	0
Injection du VLAN WiFi	0	0	0	X	0

Un ensemble de workflows est en production sur le XIQ-SE permettant d'automatiser au maximum la préparation des piles de commutateurs lors de renouvellement de matériels sans support. Ces workflows prennent en compte la personnalisation des configurations en fonction du tableau précédent site par site.

### 3.11 LISTE DES SERVEURS DU RESEAU EXTREME

Les serveurs dédiés au réseau sont virtualisés et répartis sur 3 hyperviseurs VMware ESXi version 8.0.3 avec licence vSphere 8 Essential Plus (6 CPUs 32 cœurs) représentés sur le schéma global ci-dessus. La gestion des hyperviseurs est centralisée sur VMware vCenter Server version 8.0.3 également, avec une licence vCenter Server 8 Essentials.

Les serveurs dédiés au Wifi sont virtualisés et répartis sur 2 hyperviseurs (FIDIS/ELECTRA) en VMware ESXi version 6.7.

Une évolution sur ces 3 serveurs conduite pas la DSI étant prévue vers un passage sous PROXMOX (en dehors du périmètre d'exécution du présent marché), l'offre du titulaire indique si l'ensemble des services proposés dans le cadre du poste 1 est compatible avec cette solution.

Serveurs	Versions	Licences	Fonctions	Solution de virtualisation
<b>XIQ-SE</b>	ExtremeCloudIQ-Site Engine version 25.8.11.12	2237 Pilote 90 Navigator	Administration centralisée	FIDIS VMWare ESXi 6.7u3
<b>NAC 1</b>	Virtual Access Control Engine - IA-V 25.08.10.50	12K réparties sur les 4 NACs	Authentification	Datacore VMWare ESXi 8.0.3
<b>NAC 2</b>	Virtual Access Control Engine - IA-V 25.08.10.50	12K réparties sur les 4 NACs	Authentification	Datacore VMWare ESXi 8.0.3
<b>NAC 3</b>	Virtual Access Control Engine - IA-V 25.08.10.50	12K réparties sur les 4 NACs	Authentification	FIDIS VMWare ESXi 6.7u3
<b>NAC 4</b>	Virtual Access Control Engine - IA-V 25.08.10.50	12K réparties sur les 4 NACs	Authentification	ELECTRA VMWare ESXi 6.7u3

Les licences sont saisies sur l'instance Cloud-IQ.

Les licences présentes sur XIQ-SE sont synchronisées avec l'instance Cloud-IQ.

Source	Entitlement ↑	Type	Quantity	Start Date	End Date
ExtremeCloud IQ	XIQ-NAC-S	Subscription	5,000	01/07/2025 2:00:00	01/07/2026 1:59:59
ExtremeCloud IQ	XIQ-NAC-S	Subscription	1,000	27/06/2025 2:00:00	01/07/2026 1:59:59
ExtremeCloud IQ	XIQ-NAC-S	Subscription	3,000	24/05/2025 2:00:00	24/06/2026 1:59:59
ExtremeCloud IQ	XIQ-NAC-S	Subscription	3,000	01/07/2025 2:00:00	01/07/2026 1:59:59

### 3.12 ADMINISTRATION DES EQUIPEMENTS

L'administration du réseau s'effectue à deux niveaux.

Le Service Desk, ou SD, effectue quelques opérations à l'aide du logiciel XIQ-SE et d'un profil avec des droits limités.

La cellule Réseaux Voix/Données (RVD) effectue l'ensemble de l'administration du réseau à l'aide des logiciels XIQ-SE.

Tous les équipements de la solution sont administrés en SSH et WEB au travers d'un réseau dédié (OOB) qui arrive sur des interfaces spécifiques.

### 3.13 LE PORTAIL ARTEMIX D'AUTHENTIFICATION 802.1X ET MAB

Une partie des postes de travail des utilisateurs est configurée en 802.1X ou bénéficie d'une authentification par adresse MAC (MAB).

Ils s'authentifient grâce à leurs comptes annuaire et tombent dans leur sous-réseau (grâce à un attribut x-vlan-wifi de notre annuaire LDAP). Les références des 3 serveurs d'annuaire à interroger avec un mécanisme de répartition des requêtes sont fournies dans [l'annexe 1](#).

La déclaration d'adresses MAC doit être faite en amont de la connexion puisque certaines machines n'ont pas la possibilité d'afficher une page Web.

Pour les machines compatibles Web, nous avons actuellement en production une redirection vers le portail du NAC, les utilisateurs ont alors 2 possibilités :

- S'authentifier via notre annuaire LDAP (avec leurs comptes prenom.nom) (pour afficher une doc de configuration 802.1X )
- S'authentifier en Guest (un code est alors envoyé par mail)

Attention : une adresse MAC ne pourra être saisie que dans un seul groupe à la fois.

Une adresse MAC déjà présente dans n'importe quel groupe ne pourra pas être ajoutée par un utilisateur quel qu'il soit. Il faudra d'abord que cette adresse MAC soit supprimée du groupe où elle était déjà présente avant de pouvoir l'ajouter ailleurs.

Le fonctionnement du portail est fourni en [annexe 2](#) ainsi que les détails techniques pour la reprise du code ainsi que sa maintenance.

Une nouvelle version de code a été implémenté en 2025 pour ajouter quelques fonctionnalités.

## 4 DESCRIPTION DES PRESTATIONS A REALISER

Sur ce marché, s'applique l'arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité (cf. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037436658>).

Le titulaire a fourni dans son offre un Plan d'Assurance Sécurité (PAS) selon le guide de l'ANSSI ([https://cyber.gouv.fr/sites/default/files/IMG/pdf/2010-12-03\\_Guide\\_externalisation.pdf](https://cyber.gouv.fr/sites/default/files/IMG/pdf/2010-12-03_Guide_externalisation.pdf)).

Le document PAS attendu peut, à titre d'exemple s'appuyer sur cet autre document : <https://www.makeitsafe.fr/comment-elaborer-un-plan-dassurance-securite-pas-pour-lexternalisation/>.

L'ensemble des prestations se résument à fournir aussi bien des matériels, des logiciels que de la prestation décrits dans ce chapitre.

Les prestations couvrent différents domaines technologiques nécessitant des compétences et des certifications différentes : L'architecture des réseaux LAN et WiFi est du constructeur EXTREME NETWORKS, la téléphonie fixe du site est du constructeur AVAYA et le serveur web utilise les technologies Symfony.

## 4.1 POSTE 1 : PRESTATION FORFAITAIRE

Le poste 1 concerne l'évolution de la plate-forme d'administration réseau XIQ-SE, CloudIQ, automatisation, remplacement de commutateurs et évolution de la solution Wifi et du portail captif wifi.

**Le poste 1 fait l'objet d'une offre de base et d'une variante 1 obligatoire. La variante est décrite à la fin du présent article.**

### OFFRE DE BASE

Les serveurs de virtualisation de la solution Wifi actuellement en production nommée FIDIS/ELECTRA doivent être remplacés.

Les équipements proposés doivent être suffisamment dimensionnés pour pouvoir héberger les solutions techniques proposées. Ces serveurs sont à reconduire sur site (on-premise). Il est demandé de fournir deux serveurs configurés en mode HA permettant d'avoir une évolution capacitive de 20% par rapport à l'existant.

Compte-tenu des évolutions prévues par l'Ecole, il est souhaité une solution de virtualisation sous logiciel PROXMOX sauf incompatibilité avec les VMs à installer ou autre choix du titulaire. Dans le cas d'une incompatibilité ou d'un autre choix, le titulaire aura proposé dans son offre une autre solution technique et prévu le transfert des compétences associé. Le support associé sur PROXMOX, ou solution technique équivalente, est précisé dans la réponse du titulaire et détaillé dans le chapitre maintenance.

Compte tenu de l'analyse des rapports d'usage du portail captif, la licence UCOPIA 2000 est suffisamment dimensionnée. Il est donc demandé de passer de la licence 5000 existante dans la précédente architecture à 2000 dans la nouvelle solution proposée.

Afin de conserver une haute disponibilité, le titulaire doit proposer une solution répondant aux contraintes ci-dessous :

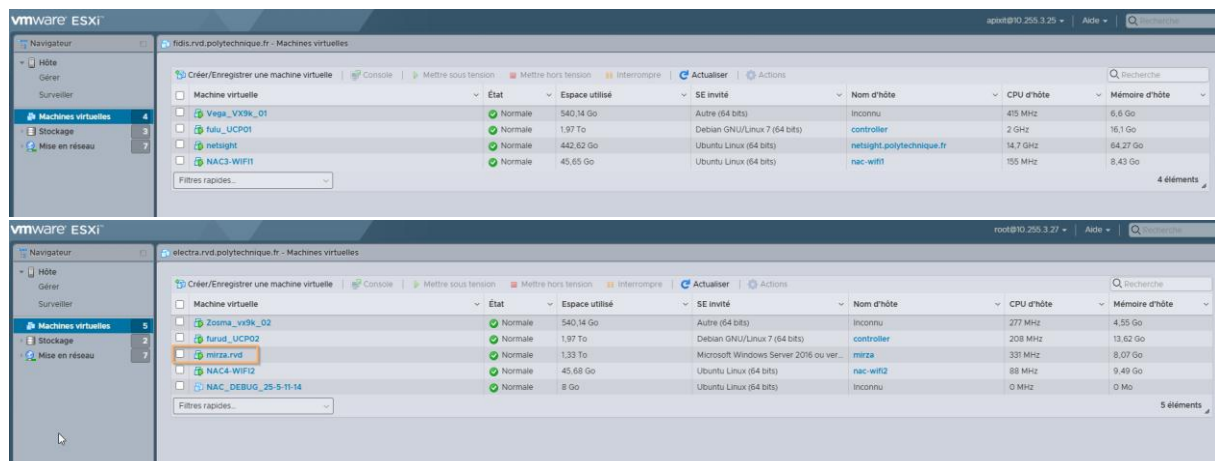
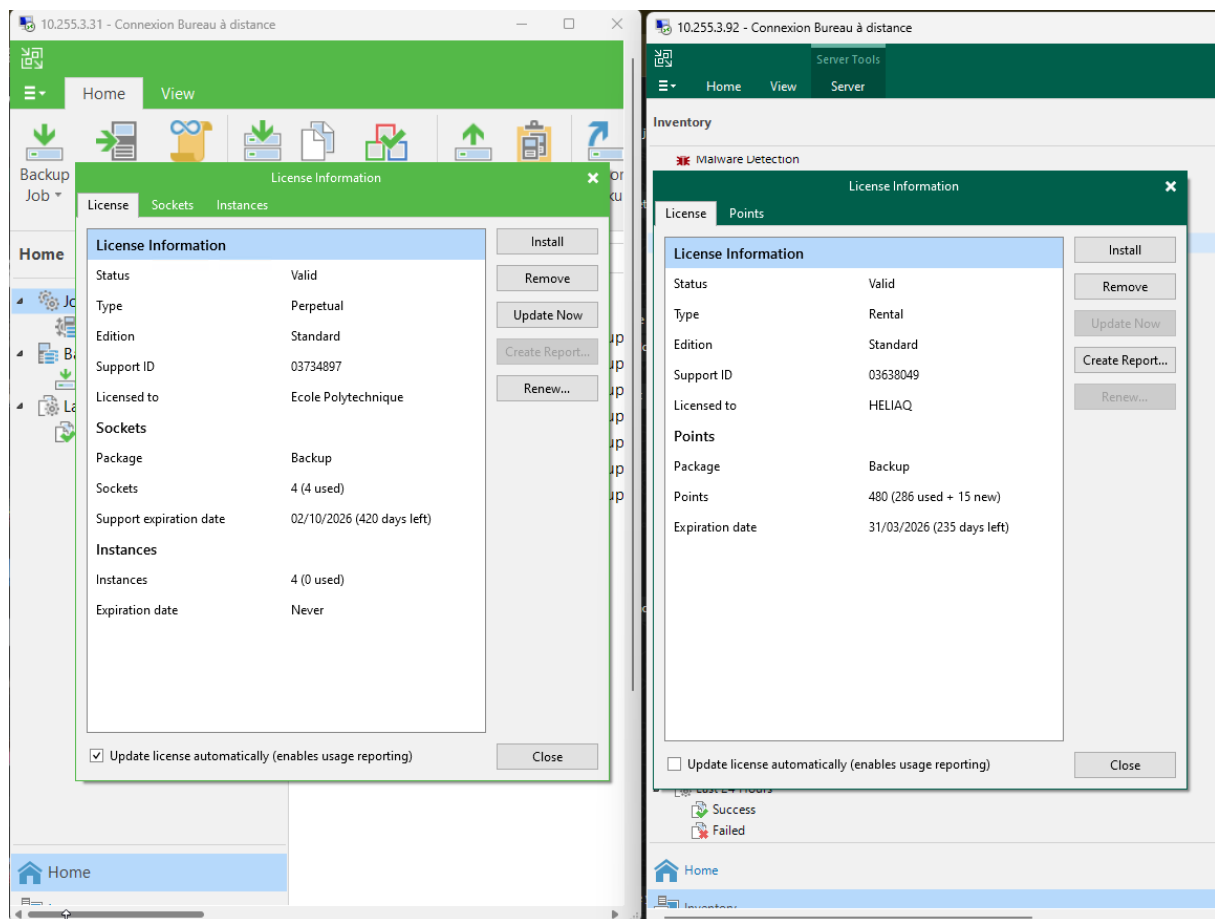
- un serveur XIQ-SE virtualisé sur site (on premise)
- un ensemble de serveurs CloudIQ virtualisé sur site (on premise),
- une solution de portail captif sur site (on premise) en cluster actif passif, de type Ucopia ou équivalent
- au moins quatre serveurs NAC en fonction du dimensionnement retenu (2 pour l'administration réseau par l'OOB, 2 pour les utilisateurs)
- **un environnement de pré-production pour les serveurs suivants : NAC, XIQ-SE et Artemix.**

Il est important de bien dimensionner le nombre de serveurs afin d'absorber un pic d'authentification sur les serveurs restants de façon non limitante. Il faut prendre en compte que d'une part le nombre de switchs authentifiant les utilisateurs va croître rapidement et qu'à partir de l'été 2026 un grand nombre de bornes (744) et les commutateurs des bâtiments élèves (2500 utilisateurs pour 650 ports) ne seront plus dans le périmètre d'authentification.

Les serveurs NACs de production sont actuellement au nombre de 4 répartis sur une solution de virtualisation indépendante (deux sur une infrastructure Datacore opérée par le pôle réseau de la DSI) et les deux autres sur FIDIS ou ELECTRA (à remplacer).

Il est demandé de proposer et de mettre en place un mécanisme natif de répartition des NAS-IP (clients du nac), de type round robin, sur les différents NACS et indiquer comment limiter au maximum les timeouts dus à la perte/mise en maintenance du NAC primaire défini sur les NAS.

Une solution de sauvegarde externe aux serveurs qui porteront les VM doit être proposée. Cette sauvegarde doit comprendre 1 réplica quotidien et 30 points de restauration en mode backup pour les VM critiques. Cette solution de sauvegarde peut être celle incluse dans PROMOX, la solution actuelle étant du Veeam, présentée ci-après.



Pour l'ensemble des points exprimés ci-après, une intégration native à XIQ-SE est à privilégier, une solution équivalente par un outil externe doit être argumentée dans l'offre du titulaire. Ce dernier doit en particulier expliciter la maintenabilité de cette brique externe en termes de suivi mise à jour, d'évolution et compatibilité y compris avec les mises à jour de la solution Extreme Networks.

Les solutions nativement proposées par la plateforme XIQ-SE sont à privilégier chaque fois que cela est possible.

La prestation doit inclure le développement d'un workflow XIQ-SE ou équivalent pour réaliser des tests de conformité de configuration de façon périodique (type journalier).

Les tests de conformité demandés, à réaliser lors de la prestation, sont les suivants :

- vérification de la présence du mécanisme dhcp snooping

- vérification de la présence du mécanisme de limit-learning
- vérification qu'un port sans display-string n'est pas UP, sinon remonter la liste des ports UP qui n'ont pas de description (display string) par stack.
- vérification des ports d'un switch : proposer une remédiation qui désactive l'ensemble des ports qui n'ont pas de description et qui ne sont pas UP. Inclure des critères de section (ou variables) comme l'appartenance le fait d'activer ou non la remédiation aussi l'appartenance à un site (XIQ-SE site) permettant de par exemple lister les ports sans les désactiver pour l'ensemble des équipements du site Enseignement (variable de site), et par contre lister et désactiver les ports répondant aux critères de l'ensemble des équipements du site Management. Le rapport doit inclure la liste des ports détectés et la liste des ports modifiés par mail.
- vérification de présence de vlan : remonter la liste des ports UP qui n'ont pas de vlan ainsi que la liste des ports qui ont une description (display string) mais aucun vlan de configuré sur le port.
- vérification de l'activation du SSH uniquement sur le VR-MGMT, sinon remonter la liste des stacks concernés, voire proposer directement une remédiation.
- vérifier la conformité du serveur NTP déclaré, sinon remonter la liste des stacks concernés.

Les remontées d'informations proposées peuvent aller jusqu'à l'envoi de mails automatiques formatées avec le minimum d'informations pour les exploiter par la suite.

La prestation doit inclure le développement d'un workflow XIQ-SE ou équivalent lorsque la vitesse d'un port du réseau passe de 2,5G à 1G à 100M ou 10M (message type vlan.msgs.portLinkStateUp).  
Voir l'exemple ci-dessous appliqué à une borne Wifi.

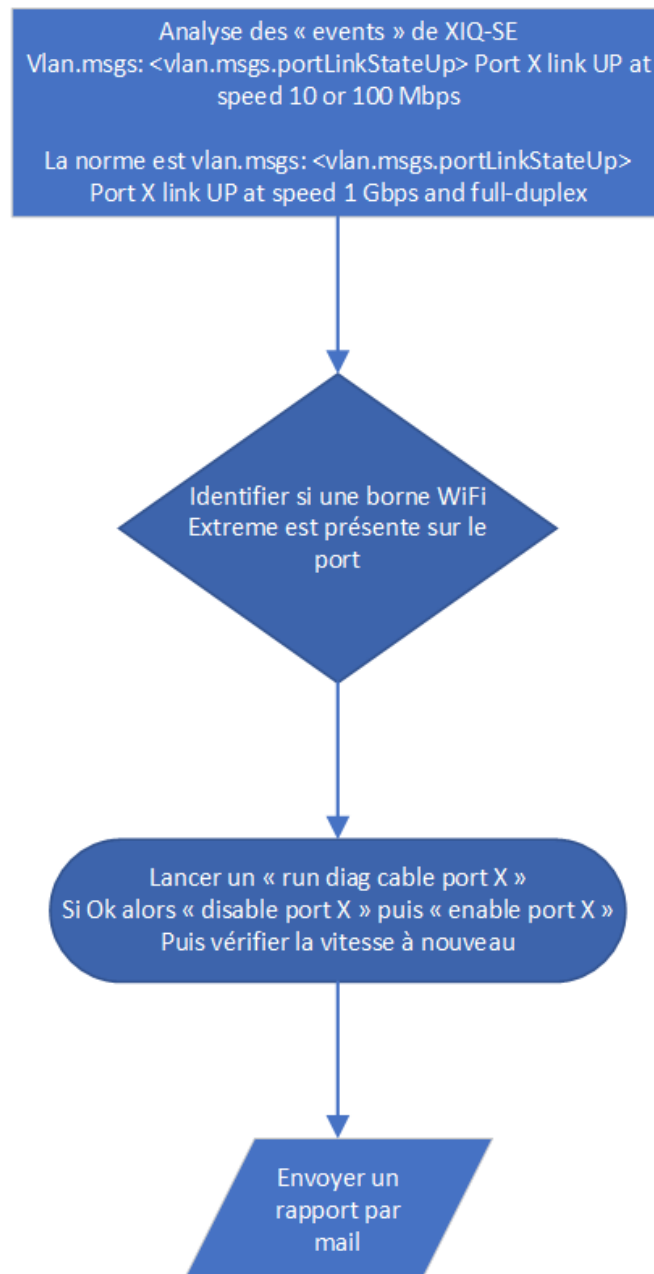


Figure 7: Diagramme du workflow d'analyse des ports WiFi

La prestation doit inclure la réalisation d'un workflow XIQ-SE ou équivalent permettant de renommer le nom d'un vlan sur toute l'infra en ne précisant en entrée que le nom de l'ancien vlan et le nouveau nom. Ceci doit s'exécuter aussi bien sur de l'XOS et du VOSS et passer des commandes sur l'ensemble des équipements où le vlan est déclaré. La prestation doit prévoir une façon de modifier les vlans définis dans les sites ou utilisés dans le process de préparation des configurations des nouveaux équipements. La prestation inclut le cas particulier des vlans dynamiques d'un switch relié en Fabric Attach dont le nom du vlan est de la forme SYS\_VLAN\_ »Tag\_du\_vlan ».

La prestation doit inclure la réalisation d'un workflow XIQ-SE ou équivalent pour remonter et tenter une remédiation intelligente lorsque des ports cuivres sensibles passent d'un état UP à DOWN. Ces changements d'état sont gérés en temps réel et si la remédiation ne fonctionne pas, un courriel est envoyé aux administrateurs réseaux indiquant le résultat de la remédiation et l'ensemble des informations pertinentes associées tel que nom de l'équipement, numéro de slot/port compteurs de changement d'état du lien du port.

La prestation doit inclure une évolution du Workflow d'XIQ-SE « Ajout-de-bornes-CloudIQ » pour rendre automatique la déclaration de l'ensemble des IP des bornes en tant que NAS-IP au niveau des NACs. Actuellement, le Workflow d'XIQ-SE injecte l'information d'un CSV contenant les numéros de série de nouvelles bornes à mettre en production dans l'interface Extreme Cloud IQ.

La prestation doit inclure un Workflow d'XIQ-SE ou équivalent permettant de lister l'ensemble des ports en production qui n'ont pas de display string (description du port).

La prestation doit inclure la réalisation d'outils permettant de généraliser l'accès Netlogin sur tous les ports utilisateurs de l'infrastructure (1000 commutateurs environ). Le titulaire doit prendre en considération, dans un premier temps, de fournir une solution permettant de collecter puis passer en MAB l'ensemble des ports puis d'assurer une migration progressive à la main de la DSI sans réaliser de blocage sur la production ou sur un temps défini. Le titulaire réalise la migration MAB d'un laboratoire pilote en lien avec le pôle réseau de la DSI.

A cet effet, la prestation doit inclure une phase de collecte des informations de type adresse matérielle (MAC) par vlan nécessaire. Il s'agit d'un prérequis en amont de l'activation du Netlogin MAC. Le mécanisme industrialisé de création des règles d'authentification (« NAC rules » du menu Control d'XIQ-SE) est aussi à prévoir au moyen d'une API ou un mécanisme équivalent. Le titulaire doit inclure un mécanisme de limitation d'adresses MAC par port/vlan. La création des groupes d'adresses mac ainsi que le peuplement de ces groupes doit se faire via l'API du portail Artemix en se basant sur la collecte décrite ci avant.

Le titulaire aura décrit dans son offre le mécanisme de montée en charge et de prévoit de développer un Workflow, un rapport, ou une intégration à la plateforme Centreon de l'Ecole polytechnique permettant d'obtenir des indicateurs sur la montée en charge des NACS (à minima nombre d'authentification simultanée) en temps réel, au quotidien, hebdomadairement et mensuellement.

#### Suppression des scripts UPM :

La prestation doit inclure un moyen centralisé (via XIQ-SE préconisé) de gestion de d'authentification des Hardphones Avaya afin de remplacer les scripts UPM qui s'exécutent localement sur les équipements de distribution.

L'activation du Netlogin sur les commutateurs de périphérie est un prérequis de cette transformation. Le titulaire a en charge la mise en oeuvre complète du Netlogin sur le parc réseau avec une phase pilote pour valider le principe de fonctionnement.

Le titulaire décrit dans son offre les étapes du processus de transformation pour un équipement où l'authentification est déjà activée ainsi que pour les équipements où le Netlogin n'a pas été encore été activé sur les équipements réseaux.

L'authentification 802.1X des téléphones Avaya doit être proposé à minima et réalisé sur un périmètre de test. La prestation doit inclure la sécurisation du téléphone physique Avaya en empêchant un accès utilisateur aux paramètres du téléphone.

La prestation doit inclure un workflow à exécuter quotidiennement de recherche d'une chaîne de caractère précise dans les logs des switches ... pour y détecter des erreurs types sur l'infrastructure et remonter un rapport d'incident par mail en cas d'anomalie et proposer un mécanisme de remédiation.

L'exemple à mettre en oeuvre est la recherche de la chaîne suivante « process CPU snmpmaster > à 80% ».

La prestation doit inclure des propositions d'évolutions fonctionnelles et de sécurisation du mécanisme de staging actuel qui se présente sous la forme de Workflow avec des input sous la forme d'un fichier CSV.

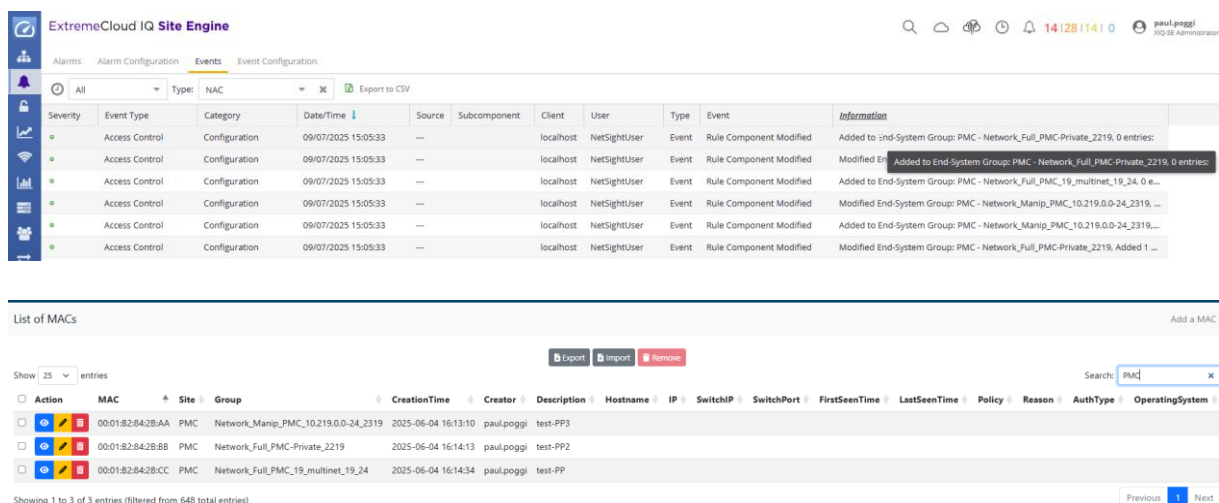
La modification du référentiel de source d'information nécessaire au fonctionnement du Workflow de Staging d'XIQ doit faire l'objet d'une proposition d'optimisation. Le Workflow de staging actuel sera à adapter en fonction de la solution proposée. Celle-ci peut s'appuyer sur l'outillage évoqué ci-après permettant d'avoir un nouveau référentiel en lieu et place d'XIQ-SE.

Ce référentiel doit se substituer à la source d'information actuelle (un fichier CSV) du Workflow de staging d'XIQ et être actualisé en temps réel par une API connectée à XIQ-SE. Le Workflow est à adapter en fonction de la solution proposée.

La prestation doit inclure une optimisation du code du portail ARTEMIX comme suit :

Au lieu d'avoir une requête par mac, il faut agréger les adresses mac par groupe et les ajouter dans un groupe avec la description associée afin d'avoir une requête par groupe. En effet, la base en production à 700 adresses MACs doit passer à 9000 à terme.

L'état actuel du code met en évidence ci-dessous un stress d'un point de vue XIQ-SE :

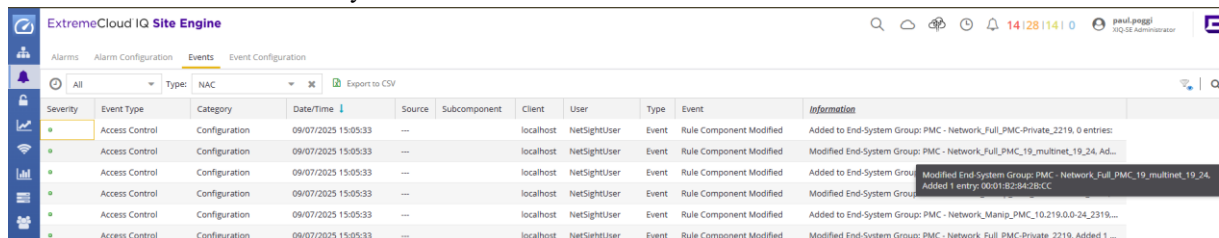


The screenshot shows the ExtremeCloud IQ Site Engine interface. At the top, there's a navigation bar with 'Alarms', 'Alarm Configuration', 'Events', and 'Event Configuration'. Below this, there's a search bar and a table of events. The table has columns: Severity, Event Type, Category, Date/Time, Source, Subcomponent, Client, User, Type, Event, and Information. The 'Information' column contains details about rule component modifications and system group additions. Below the table, there's a section titled 'List of MACs' with a search bar and a table of MAC addresses. The table has columns: Action, MAC, Site, Group, CreationTime, Creator, Description, Hostname, IP, SwitchIP, SwitchPort, FirstSeenTime, LastSeenTime, Policy, Reason, AuthType, and OperatingSystem. The table shows three entries for MAC addresses 00:01:82:84:2B:AA, 00:01:82:84:2B:BB, and 00:01:82:84:2B:CC, all associated with the 'PMC' site and 'Network\_Manip\_PMC' group.

Severity	Event Type	Category	Date/Time	Source	Subcomponent	Client	User	Type	Event	Information
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:

Action	MAC	Site	Group	CreationTime	Creator	Description	Hostname	IP	SwitchIP	SwitchPort	FirstSeenTime	LastSeenTime	Policy	Reason	AuthType	OperatingSystem
	00:01:82:84:2B:AA	PMC	Network_Manip_PMC_10.219.0.0-24_2319	2025-06-04 16:13:10	paul.poggi	test-PP3										
	00:01:82:84:2B:BB	PMC	Network_Full_PMC-Private_2219	2025-06-04 16:14:13	paul.poggi	test-PP2										
	00:01:82:84:2B:CC	PMC	Network_Full_PMC_19_multinet_19_24	2025-06-04 16:14:34	paul.poggi	test-PP										

Problème : le add renvoie 0 entry



The screenshot shows the ExtremeCloud IQ Site Engine interface. At the top, there's a navigation bar with 'Alarms', 'Alarm Configuration', 'Events', and 'Event Configuration'. Below this, there's a search bar and a table of events. The table has columns: Severity, Event Type, Category, Date/Time, Source, Subcomponent, Client, User, Type, Event, and Information. The 'Information' column contains details about rule component modifications and system group additions. Below the table, there's a section titled 'List of MACs' with a search bar and a table of MAC addresses. The table has columns: Action, MAC, Site, Group, CreationTime, Creator, Description, Hostname, IP, SwitchIP, SwitchPort, FirstSeenTime, LastSeenTime, Policy, Reason, AuthType, and OperatingSystem. The table shows three entries for MAC addresses 00:01:82:84:2B:AA, 00:01:82:84:2B:BB, and 00:01:82:84:2B:CC, all associated with the 'PMC' site and 'Network\_Manip\_PMC' group.

Severity	Event Type	Category	Date/Time	Source	Subcomponent	Client	User	Type	Event	Information
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Added to End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:
	Access Control	Configuration	09/07/2025 15:05:33	---		localhost	NetSightUser	Event	Rule Component Modified	Modified End-System Group: PMC - Network_Full_PMC-Private_2219, 0 entries:

Action	MAC	Site	Group	CreationTime	Creator	Description	Hostname	IP	SwitchIP	SwitchPort	FirstSeenTime	LastSeenTime	Policy	Reason	AuthType	OperatingSystem
	00:01:82:84:2B:AA	PMC	Network_Manip_PMC_10.219.0.0-24_2319	2025-06-04 16:13:10	paul.poggi	test-PP3										
	00:01:82:84:2B:BB	PMC	Network_Full_PMC-Private_2219	2025-06-04 16:14:13	paul.poggi	test-PP2										
	00:01:82:84:2B:CC	PMC	Network_Full_PMC_19_multinet_19_24	2025-06-04 16:14:34	paul.poggi	test-PP										

Voir à cet effet le script existant en [annexe 3](#) du présent document.

La prestation doit inclure un outillage de plusieurs logiciels permettant d'avoir un état temps réel du parc en production (Lan et Wifi) dans une base de données (type Netbox/Budybase/N8N et/ou équivalent). Il s'agit de s'appuyer sur les données de la brique XIQ-SE pour que l'outil puisse permettre au pôle réseau de la DSI d'exploiter la valorisation financière du parc, gérer l'obsolescence, les dates de mises à jour, etc... permettant de construire des indicateurs fiables au quotidien. La prestation doit inclure l'optimisation du fonctionnement actuel des workflows décrits dans [l'annexe n°6](#) servant de guide pour renouveler, en masse, les piles de commutateurs lors des remplacements via le schéma directeur informatique.

Gestion des clefs radius :

La prestation doit inclure la mise en place d'une solution de type VAULT ou un équivalent pour répondre à des exigences de sécurité sur la gestion des clefs radius. Ces clés sont utilisées pour la configuration automatique des switch dans le Workflow de staging d'XIQ-SE. Actuellement, ces clefs sont stockées dans des fichiers texte hébergés en read-only sur le serveur XIQ-SE.

Le titulaire fournit dans son offre une analyse critique de la configuration Wifi CloudIQ actuellement en production en fonction de [l'annexe technique n°4](#), notamment sur les profils radio et les policy.

La prestation doit inclure un livrable global d'exploitation et de maintenance de tout l'outillage réalisé de ce chapitre. Pour accompagner ce projet et permettre à l'équipe réseau de la DSI de garder la maîtrise des nouveaux outils et développements, une ou plusieurs formations et un ou plusieurs transferts de compétences sont réalisés par le titulaire. L'offre du titulaire inclut une formation de 5 jours minimum. Celle-ci est réalisée deux fois, avec un public de 4 personnes par session. Le titulaire détaille dans son offre le programme des formations et/ou transferts de compétences.

#### ***VARIANTE 1 OBLIGATOIRE : infrastructure dans le cloud***

*La variante porte sur la mise à disposition de la même infrastructure décrite précédemment dans le Cloud au lieu d'être intégralement on premise.*

*Le service Cloud de la variante concerne uniquement le service nommé CloudIQ, les services NACs, XIQ-SE, portail captif Wifi et Artemix restant eux sur les serveurs prévus dans l'offre de base.*

## **4.2 POSTE 2 : PRESTATIONS A BON DE COMMANDE**

### **4.2.1 MAINTENANCE MATERIELLE ET LOGICIELLE DU PARC**

**La maintenance matérielle et logicielle fait l'objet d'une offre de base et d'une variante 2 obligatoire. La variante est décrite à la fin du présent article.**

#### **OFFRE DE BASE**

**Les adossements au constructeur EXTREME NETWORKS sont à fournir annuellement, à date anniversaire de la notification.**

La maintenance s'applique sur l'ensemble des matériels et logiciels décrit dans ce document.

Le bordereau de prix unitaires permet de commander :

- La maintenance annuelle ou sur une période de 3 ans correspond au parc existant (défini à [l'annexe 5](#)) au moment de la notification du marché (selon évolutions liées aux fins de supports des matériels),
- La maintenance annuelle ou sur une période de 3ans supplémentaire correspond uniquement au périmètre du poste 1.

Le titulaire ne peut invoquer après notification du marché sa méconnaissance de telle ou telle caractéristique des lieux, matériels ou logiciels.

L'offre du titulaire doit inclure dans le chiffrage de la maintenance un accès à une hotline et les télé-interventions nécessaires au diagnostic des pannes. L'ensemble du service de maintenance doit être accessible 5/7j de 8h à 18h par la hotline fournie au titre du marché. La garantie de temps d'intervention est de 8 heures dès la déclaration d'une panne à la hot-line.

La prestation doit inclure la correction des versions logicielles en place en cas de bogue rencontré sur les logiciels existants.

**En cas de panne matérielle (exemple : tout type de modules des VSP, etc ...), lorsque le matériel est déclaré défectueux par l'ouverture d'un appel ou d'un ticket à la hotline, il doit être remplacé sur site sous J+1 (GTR).**

Le maître d'ouvrage impose une garantie de temps d'intervention de 8 heures ouvrées et une garantie de temps de rétablissement en conditions opérationnelles au jour ouvré suivant sur les éléments objet du poste n°1.

Le paiement de la facture de maintenance reste soumis à la fourniture de la preuve de réassurance du titulaire auprès du constructeur de ladite maintenance.

La maintenance des matériels et/ou accessoires commandés au titre du poste à bon de commande est commandée, le cas échéant, à partir du bordereau de prix du même poste.

Conformément à la clause de réexamen renseignée au CCAP, les matériels et/ou logiciels peuvent être retirés de la maintenance en fonction de leur date de fin de support annoncée par le constructeur ou de l'arrêt des équipements et/ou du service par la Direction des Systèmes d'Information de l'École polytechnique.

Dans le cadre de la maintenance, l'École polytechnique fournit soit un VPN site à site, soit un usage de la solution VPN interne Global Protect de Palo Alto au titulaire. Cet accès VPN est ouvert à la demande du titulaire uniquement.

L'usage du VPN requérant un compte nominatif dans l'annuaire de l'École, le titulaire du marché doit remplir les annexes de clause de confidentialité d'accès au système d'information.

L'ensemble des contrats de maintenance à reprendre sont présents dans [l'annexe n°5](#). Ces contrats incluent l'accès au service premier du constructeur qu'il convient de reconduire. Les items sans support ne seront pas à reconduire dans l'offre financière (exemple : bornes 7632).

Description du service premier :

Accès complet au Global Technical Assistance Center (GTAC) : 24/7/365, gestion prioritaire, ouverture de tickets multicanale.

Fourniture d'un interlocuteur unique chargé du suivi, de l'escalade et du reporting (nommé Premier Delivery Manager) incluant une réunion bi-hebdomadaire de suivi.

Le service Premier contient 2 audits de santé du réseau par an (1 sur le Lan, 1 sur le Wifi), rapports détaillés, recommandations techniques, réunion triannuelle.

Accès complet aux mises à jour, correctifs, versions majeures et mineures.

Priorisation des tickets Premier, ingénieurs certifiés, escalade R&D si nécessaire.

Les SLA – Délais de prise en charge – sont les suivants :

S1 critique : 15 min

S2 dégradé : 1 h

S3 mineur : 4 h

#### ***VARIANTE 2 OBLIGATOIRE : maintenance au format EPI***

Dans le cadre de la variante, les contrats sont convertis au nouveau format de licence nommé Extreme platformOne (EP1) afin de bénéficier d'un contrat de type ENTERPRISE agreement.

---

### **4.2.2 SOLUTION LOAD BALANCER**

Le titulaire propose au bordereau de prix unitaires une solution de load-balancer redondée (un cluster de 2 matériels) pour pouvoir répartir le trafic utilisateur sans latence entre les différents serveurs NACs. Cette solution doit permettre d'assurer une redondance des serveurs NACs sans latence et permettre également de rester en capacité d'authentifier l'ensemble des flux utilisateurs en cas de perte d'un ou plusieurs serveurs NAC. Le titulaire intègre l'ensemble des prestations dont l'étude de l'architecture, la configuration des matériels proposés et des modifications à réaliser sur l'existant (commutateurs réseaux et bornes Wifi inclus), des tests de recette et une mise en production. Le titulaire précise dans son offre si la solution peut être installée dans deux salles informatiques distinctes (distante de plus de 500m) et les prérequis nécessaires au déploiement.

---

#### 4.2.3 UNITE D'ŒUVRES

Pour faire évoluer l'architecture, la DSI est susceptible d'avoir recours à des prestations de haute technicité pour la mise en œuvre de nouvelles fonctionnalités ou expertise sur des problèmes auxquels elle devrait faire face.

Les types de prestations sont renseignées au BPU. Les prestations du constructeur EXTREME NETWORKS sont demandées en appui des ressources du titulaire.

---

#### 4.2.4 ACCESSOIRES ET LICENCES

Le titulaire a complété le BPU (bordereau de prix unitaires) remis dans son offre avec des références liées aux produits proposés dans le cadre du poste n°1 et de la maintenance.

Il peut s'agir de composants matériels ou logiciels liés au constructeur EXTREME NETWORKS aussi bien en réseau qu'en Wifi.

Il est demandé également la fourniture de tout accessoire ou logiciel proposé dans la réponse du titulaire.

## 5 TABLES DES FIGURES

Figure 1: Schéma structurel du réseau de l'Ecole Polytechnique .....	11
Figure 2: Schéma des flux d'authentification du SSID eduroam .....	14
Figure 3: Schéma des flux d'authentification sur le portail captif du SSID Guest.....	15
Figure 4: Schéma de flux d'authentification par adresse MAC sur le SSID BYOD .....	16
Figure 5: Schéma global des flux d'authentification WiFi WiNG et CloudIQ .....	17
Figure 6. Localisation sur le campus polytechnique des quatre LTP .....	20
Figure 7: Diagramme du workflow d'analyse des ports WiFi.....	29

## 5.1 ANNEXES

**Les annexes sont disponibles dans le dossier archive sécurisé joint au DCE.**

ANNEXE 1 : Connexion à l'annuaire LDAP d'entreprise

ANNEXE 2 : Documentation du portail web ARTEMIX

ANNEXE 3 : Optimisation des requêtes du portail web ARTEMIX

ANNEXE 4 : Configuration CloudIQ

ANNEXE 5 : Liste des contrats de maintenance à reprendre

ANNEXE 6 : Guide des Workflows XIQ-SE en production

ANNEXE 7 : Les 3 scripts UPM utilisés sur nos switchs pour la téléphonie