

Référentiel technique des infrastructures informatiques des lycées

Référentiel technique des infra info des lycées

Contacts

Nom	Société	Fonction	Téléphone	Courriel
Laurent Couillaud	Vice-Rectorat	Technicien BISR	26 61 35	laurent.couillaud@ac-noumea.nc

Révision du document

Version	Date de modification	Auteur	Description
1.0	26/10/2016	Laurent Couillaud	Documentation initiale
1.1	2/06/2017	Laurent Couillaud	Ajout détail fibre optique

Validation du document Version

	Nom	Fonction	Date
Validation par :	Gilles Leroi	Chef de la DSI	2/06/2017

Table des matières

Introduction.....	4
I.Architecture.....	5
<i>A.Les zones.....</i>	<i>5</i>
<i>B.Les règles de filtrage.....</i>	<i>6</i>
II.Infrastructure.....	7
<i>A.Architecture type d'établissement.....</i>	<i>7</i>
<i>B.Les locaux techniques.....</i>	<i>7</i>
1.Le local technique principal :.....	7
2.Les locaux techniques secondaires :.....	7
3.Remarques.....	7
<i>C.Protection et continuité électrique.....</i>	<i>8</i>
<i>D.Le câblage physique.....</i>	<i>8</i>
<i>E.Le routeur pour l'accès Internet.....</i>	<i>9</i>
<i>F.Les commutateurs.....</i>	<i>9</i>
<i>G.Les bornes et le contrôleur Wi-Fi.....</i>	<i>9</i>
<i>H.La segmentation du réseau en Vlan.....</i>	<i>11</i>
<i>I.Les tablettes.....</i>	<i>13</i>
<i>J.La vidéosurveillance.....</i>	<i>13</i>
<i>K.Les serveurs.....</i>	<i>14</i>
<i>L.L'espace de sauvegarde.....</i>	<i>14</i>
<i>M.Les services.....</i>	<i>14</i>
<i>N.Les périmètres de responsabilités.....</i>	<i>16</i>
<i>O.Nommage des équipements.....</i>	<i>18</i>
III.L'espace numérique de travail (ENT).....	18

Introduction

Depuis 2003, la mise en réseau des établissements scolaires de Nouvelle-Calédonie est une priorité du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements.

L'architecture étant devenue obsolète, son évolution est apparue indispensable afin de correspondre au mieux au développement des usages des technologies de l'information et de la communication, améliorant l'efficacité pédagogique et administrative.

Ce développement qui mobilise des ressources humaines et financières importantes, doit, dans un souci de performance, être formalisé et organisé rigoureusement.

Il est donc nécessaire de réfléchir à des solutions techniques et d'organisation communes et standardisées pour faciliter la mise en place de ces réseaux et leur maintenance.

Ces solutions sont ici présentées sous la forme d'un **schéma directeur** à destination des établissements et des partenaires.

Ces recommandations constituent pour certains aspects une base de discussion, pour d'autres, un référentiel et un engagement du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements à assurer le suivi des solutions évoquées.

L'évolution technologique d'une part, l'introduction d'un nouveau système de téléphonie dans les établissements d'autre part, nous a amené à remanier l'architecture actuelle et proposer une nouvelle mouture du réseau en prenant en compte la virtualisation des serveurs.

I. Architecture

A. Les zones

Les services du vice-rectorat préconisent une architecture type respectant les règles d'accès **aux réseaux AGRIATES et RACINE et les politiques de sécurité académique et locale**.

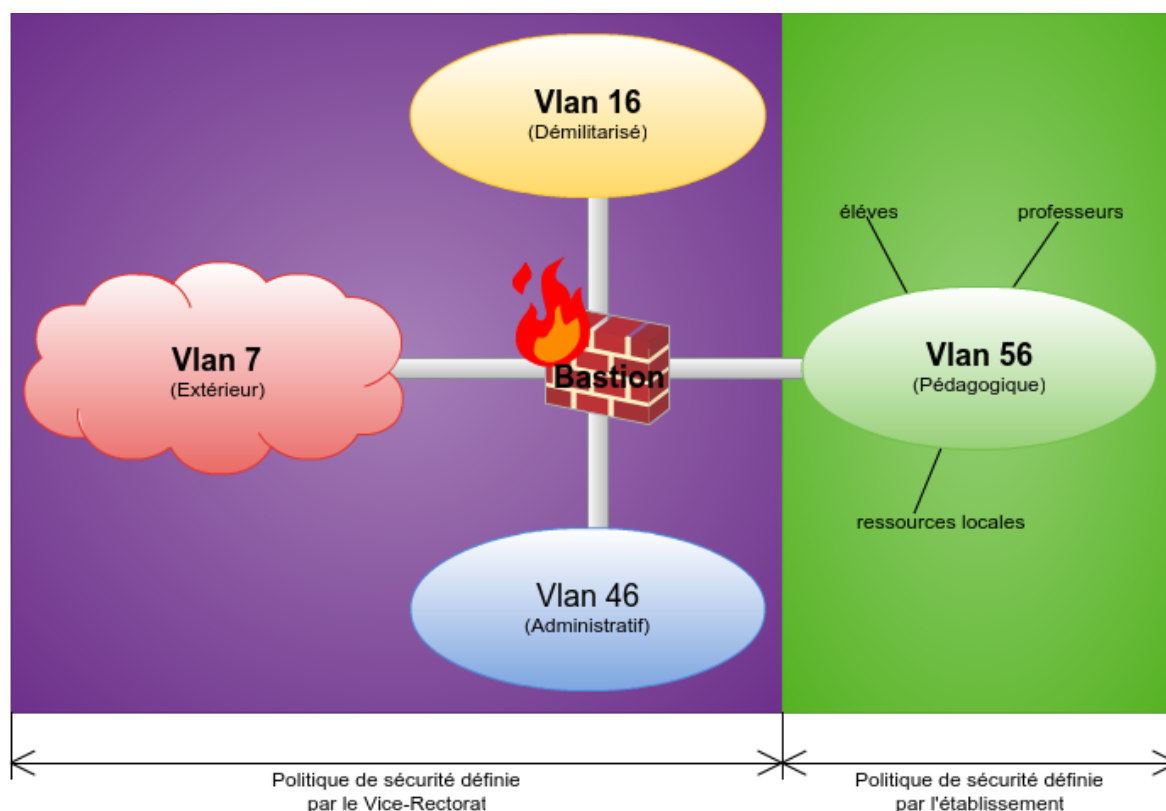
Notamment il conviendra de respecter l'ensemble des dispositifs à prévoir dans le cas de la mise en place des « Services numériques et protection des mineurs » : <http://eduscol.education.fr/cid57087/textes-officiels-et-preconisations.html>.

Il s'agira notamment de filtrer les accès à Internet et de conserver pendant 1 an les traces des usagers. (cf **Annexe 7**).

Cette architecture se décline en plusieurs zones en fonction des technologies installées dans l'établissement. Ces zones doivent être séparées par au moins une passerelle de sécurité. Elles seront constituées d'un réseau LAN segmenté en VLAN :

- Le VLAN 7 (Internet) doit être l'unique accès Internet pour le réseau administratif et pédagogique.
- Le VLAN 16 (DMZ publique et privé) est la zone dite « démilitarisée » permettant l'ouverture et le partage sécurisé des ressources de l'établissement (Pronote, ENT...).
- Le VLAN 56 (Pédagogie) est la zone d'enseignement réservée aux personnels enseignants, aux élèves et aux étudiants.
- Le VLAN 46 (Administratif) est la zone d'accès à tous les agents administratifs de l'établissement (ayant des droits défini par le chef d'établissement).

La passerelle de sécurité est assurée par le module AMON du projet EOLE. Il assure le rôle de pare-feu, filtrage d'URL et de routage entre les précédentes zones.



Référentiel technique des infra info des lycées

B. Les règles de filtrage

Les règles de filtrage doivent respecter le tableau suivant :

De → Vers	Vlan 7 (Internet)	Vlan 16 (Démilitarisé)	Vlan 56 (Pédagogie)	Vlan 46 (Administratif)	BASTION
Vlan 7 (Internet)		Interdit	Interdit	Interdit	Interdit
Vlan 16 (Démilitarisé)	Autorisé		Contrôlé	Contrôlé	Interdit
Vlan 56 (Pédagogie)	Contrôlé	Autorisé		Interdit	Interdit
Vlan 46 (Administratif)	Contrôlé	Autorisé	Autorisé		Interdit
BASTION	Autorisé	Autorisé	Autorisé	Autorisé	

Autorisé	: Tous les flux sont autorisés par défaut.
Contrôlé	: Certains flux sont prédéfinis ou autorisés après demande et validation de la DSI
Interdit	: Tous les flux sont interdits

BASTION : La zone bastion correspond au serveur Amon.

II. Infrastructure

A. Architecture type d'établissement

Un schéma de l'architecture type est présenté en Annexe 1

B. Les locaux techniques

1. Le local technique principal :

Il est indispensable de rassembler tous les serveurs dans un seul local dédié (salle serveur type en Annexe 2), pour des raisons de sécurité et de maintenance. Les serveurs, une fois configurés, ne nécessitent pas d'intervention directe : ils sont accessibles depuis les postes clients du réseau administratif (configuration, installation/désinstallation de programmes, maintenance,...).

Ce local serveur devra être accessible uniquement par le chef d'établissement ou une personne qu'il aura habilité.

Les caractéristiques du local principal sont les suivantes :

- Choisi au sein de la structure administrative de l'établissement
- 8 m² minimum
- une porte d'accès fermant (à clé unique (pas de « passe général »), carte magnétique, carte à puce ou digicode mécanique)
- un système de climatisation : par split (redondance demandée), à réarmement automatique, avec redémarrage automatique (après coupure électrique)
- deux armoires de brassage minimum fermant à clef (une pour les serveurs et une ou plusieurs pour le brassage informatique)
- un éclairage d'au moins 500 lux
- éloignement de toutes sources de perturbations électriques
- une borne de raccordement à la terre principale
- des alimentations avec différentiel de 30 mA dédié en fonction des besoins
- les composantes de sécurité électrique des serveurs (onduleur et/ou réseau électrique ondulé)
- les commutateurs et routeur ADSL ou FTTH
- le point de communication Internet (ligne ADSL ou routeur FO OPT)
- la tête de lignes OPT
- Alimentation électrique suffisante (préconisation : réseau électrique ondulé)
- Accès sécurisé (porte, fenêtres avec rideau ignifugé ou film solaire)
- **utilisation exclusive à cet effet**

2. Les locaux techniques secondaires :

Les caractéristiques des locaux techniques secondaires sont les suivantes :

- Une surface de 4 m² minimum
- un éclairage d'au moins 500 lux
- une alimentation avec différentiel de 30 mA dédié
- un composant de sécurité électrique des éléments actifs (onduleur)
- un système d'aération efficace
- 1 prise électrique en plus de celles intégrées dans l'armoire de brassage pour y brancher éventuellement un analyseur de réseau, un équipement en test, etc.
- un raccordement au réseau de mise à la terre
- éloignement de toutes sources de perturbations électriques
- un sous répartiteur sous forme d'armoire avec panneaux de brassage RJ45 fermant à clef
- **utilisation exclusive à cet effet**

3. Remarques

Ces recommandations devront être totalement respectées dans le cas de bâtiments neufs ou rénovés (la prise en compte

Référentiel technique des infra info des lycées

doit se faire au moment de l'élaboration du cahier des charges pour la conception du bâtiments).

Cas des bâtiments anciens : Autant que faire se peut, on devra respecter ces recommandations. On peut admettre que dans le cas d'un répartiteur de moins de 48 prises terminales, celui-ci peut être situé dans une pièce attribuée à d'autres fonctions, à condition que le répartiteur et équipements soient installés dans une armoire ondulée et fermée à clef, de préférence hors de portée des utilisateurs (au dessus d'une porte, dans une salles de repos ou une salle de professeurs).

C. Protection et continuité électrique

Prévoir une protection et une continuité électrique via un onduleur pour chaque baie de brassage.

L'onduleur devra parer aux surintensités, court-circuits, surtensions, sous-tensions et déchargement excessif de la batterie.

D. Le câblage physique

Dans la perspective de permettre à tous les acteurs, pédagogiques et administratifs, d'accéder à des ressources, il est nécessaire d'envisager la conception du câblage de façon globale et évolutive.

L'étude et la mise en place du lien physique de raccordement de tous les ordinateurs au local serveur doivent prendre en considération non seulement les besoins de liaison immédiats, mais également ceux que les évolutions technologiques feront progressivement émerger.

Le réseau doit assurer en termes de communication, une qualité suffisante pour répondre aux exigences des prochaines années. Il est donc préconisé de choisir les ressources afin de garantir un débit de 1Go/s constant dans l'ensemble de ses composantes :

- Câble de type paire torsadée (F/FTP) de catégorie 6a avec certification, et connecteurs RJ45 ;
- Interconnexion de type « commutateur Fast Ethernet ».
- 2 types de commutateurs obligatoirement manageables :
 - Commutateur de coeur de réseau de niveau 3 (local principal), ports 10 000 Mbps. Principalement des ports fibres optiques.
 - Commutateur d'accès de niveau 2 (locaux secondaires) avec des ports 1 000 Mbps.
Possibilité d'installer des commutateurs 24 ports POE (Power Over Ethernet). Le POE permet d'alimenter électriquement les bornes Wifi et les téléphones par le câble Ethernet.
- Agrégations des fibres optiques pour permettre une répartition de charge ;
- Epissure des fibres optiques pour permettre une continuité et une distribution exclusive de chaque baie ;
- 6 brins minimum par baie informatique ;
- Carte réseau de chaque ordinateur de type Ethernet 1 000 Mbps.

Les distances supérieures à **90 mètres** seront réalisés en fibre optique. Les raccordements entre les bâtiments sont résolus par la mise en place de lignes primaires en fibre optique sur lesquelles pourront se connecter les différentes salles, au fur et à mesure des besoins et des budgets. Pour des raisons de masse électrique, il faut connecter tous les bâtiments entre eux quel que soit la distance qui les relie avec de la fibre. Si le bâtiment s'avère relié par du cuivre, il faut qu'il y ait absolument une mise à la terre commune.

Le câblage constitue un réseau physique unique connecté à l'armoire de brassage du local serveur. Il couvre l'ensemble des zones devant être équipées en informatique et/ou en téléphonie. Dans ce dernier cas, pour des raisons d'accessibilité ou de couverture, le câblage filaire (cuivre ou FO) peut être complété par des balises sans-fil de type DECT permettant d'assurer les services de téléphonie.

La DSI recommande que les cordons de brassages soient fournis avec des bagues d'identification de réseau de couleurs :

- Vert : réseau pédagogique
- Bleu : réseau administratif
- Jaune : réseau public (DMZ)
- Rouge : accès extérieur Internet

Référentiel technique des infra info des lycées

E. Le routeur pour l'accès Internet

Les établissements scolaires sont actuellement dotés d'un routeur ADSL de type CISCO séries 800. Le modèle CISCO séries 877 n'étant plus commercialisé, la DSI déploie le modèle 887VA-M-K9 sans wifi.

Nous recommandons aux établissements scolaires publics raccordés à Internet via le FAI Lagoon (suite convention avec le vice-rectorat) pour le réseau administratif d'utiliser une offre dite STRATO+ (Connexion illimitée avec débit prioritaire en cas de saturation exceptionnelle du réseau Internet).

Pour les établissements pouvant être raccordés au FTTH, la DSI fournit un routeur CISCO ISR 4321/K9 configuré par ses soins.

F. Les commutateurs

Les établissements scolaires sont principalement dotés de commutateurs de type Cisco.

Les équipements de réseau doivent permettre de gérer des VLAN de type VDI (Voix Données Images) et doivent être manageables et stackables. Ils doivent en particulier pouvoir mettre en œuvre des qualités de service différentes selon le type de communication (priorité plus élevée accordée aux applications temps-réel telles que la voix sur IP).

Il est recommandé d'utiliser des switchs POE pour assurer l'alimentation électrique d'un « élément actif » via le câble informatique. Les « éléments actifs » sont par exemple les bornes Wifi, téléphones IP, caméras, boîtiers ATA (pour les alarmes de type incendie, intrusion, climatiseur, onduleur et frigos, ouverture portail à distance ...) et autres capteurs.

Il conviendra de distinguer les commutateurs de cœur de réseau (local principal) des commutateurs d'accès (locaux secondaires).

Ils devront également faire l'objet d'un étiquetage et d'un nommage selon la nomenclature définie (cf. rubrique O nommage des équipements).

L'installation et le matériel doivent être garantis sur site par l'entreprise :

- Câblage et connecteur 5 ans
- Commutateurs et autres éléments actifs 3 ans

Le câblage doit faire l'objet d'une recette de câblage.

Une fois toutes les prises testées et réparées, un rapport devra être fourni à l'établissement et la DSI. Les schémas détaillés du câblage et des armoires, les références de toutes les prises et connexions doivent être disponibles à la fin des travaux et être remis à l'établissement et une copie à la DSI.

Pour des raisons de cohérence et de compatibilité, l'ensemble des équipements réseau devra faire l'objet d'une validation technique préalable auprès de la DSI.

G. Les bornes et le contrôleur Wi-Fi

Au regard des expérimentations de la DSI, nous recommandons d'utiliser le matériel UNIFI.

L'intégration du réseau sans-fil sur les infrastructures académiques doit respecter des conditions de sécurité adaptées à l'accès aux ressources internes du système d'information.

Ainsi, vous trouverez ci-dessous les principes de déploiement du Wi-Fi définie par la **circulaire DPMA A3/MB n°2006-0098 du 18 mai 2006** :

- Obligation de signalement de la mise en place d'une borne Wi-Fi
- Confinement des accès Wi-Fi (sur une zone du réseau isolée de toutes autres ressources sensible sécurisé par un pare-feu)
- Authentification des postes de travail et des utilisateurs (borne intégrant les protocoles 802.11i / WPA2 ou versions évoluées associés à une authentification de l'utilisateur de type EAP/RADIUS)
- Fourniture éventuelle d'un service d'accès de type Hot Spot

Référentiel technique des infra info des lycées

- Modalités d'accès aux ressources internes du systèmes d'information (réseau impression...)
- L'accès aux ressources extranet (messagerie, ENT...)

D'un point de vue juridique et pour répondre aux problématiques de responsabilités en matière d'infrastructure Wi-Fi, deux pistes sont dégagées : le contenu transitant sur le réseau et l'infrastructure réseau.

Vous trouverez en **Annexe 3** de la circulaire, un document expliquant les responsabilités d'un service ou d'un établissement dans le cadre de la mise en place d'un réseau Wi-Fi.

Infrastructure :

L'implantation et le nombre de points d'accès Wi-Fi devra tenir compte du nombre d'utilisateurs et de la zone à couvrir (m², cloisonnement) ainsi que de l'usage du réseau sans fil.

Une étude préalable sera nécessaire pour définir l'équipement à installer.

Le nombre de points d'accès Wi-Fi sera défini par rapport :

- **au nombre d'utilisateurs connectés.** Le titulaire apportera une attention particulière aux bornes situées dans les zones à forte densité (hall, cour de récréation, salle de restauration, salle de cour et amphithéâtre).
- **Au périmètre à couvrir.** Le réseau Wi-Fi devra couvrir totalement ou partiellement les bâtiments (ex : uniquement les salles espaces communs, les espaces communs et quelques salles de cours).
- **Le titulaire devra prévoir un maillage pour la couverture adapté aux espaces.** Il s'agira par exemple :
 - un point d'accès tous les 15 mètres pour les espaces intérieurs cloisonnés (couverture d'environ 225 m²),
 - un point d'accès tous les 20 mètres pour les espaces intérieurs ouverts (couverture d'environ 440 m²).

Authentification (mots de passe des comptes Scribe) et chiffrement :

L'authentification au réseau Wi-Fi s'effectuera via l'accès à l'annuaire Scribe. Dès lors, il est nécessaire que l'établissement veille à l'utilisation de mots de passe (élèves, professeurs, ...) robustes. Ainsi, conformément à l'**Annexe 4** il conviendra de définir pour chaque compte d'accès au Scribe un mot de passe de 8 caractères minimum. Ce mot de passe sera composé de lettres en minuscules, majuscules et de chiffres.

Par ailleurs, la méthode de chiffrement doit utiliser des certificats à placer sur les équipements ou éventuellement une clé de cryptage (WPA2 d'une longueur minimale de 128 bits) et remis exclusivement au chef d'établissement.

Les bornes et contrôleur Wi-Fi devront :

- Etre manageable.
- Etre connectée à un port Gigabit sur un switch manageable. L'alimentation sera réalisée en POE (selon norme IEEE 802.3 af). La distance entre le point d'accès et le switch sera de maximum 90 mètres.
- Permettre la définition d'un réseau privé avec clé WPA2 et étant capable de supporter une authentification centralisée via le protocole 802.1x (RADIUS).
- Permettre la définition de minimum 4 Vlan.
- Permettre la définition de minimum 4 SSID.
- Intégrer une programmation horaire individuelle de mise en veille. Cette programmation sera définie avec l'établissement scolaire afin d'offrir une économie énergétique et une sécurité accrue à l'intrusion.
- La certification de sécurité de la part de l'ANSSI pour l'usage d'un contrôleur Wi-Fi est recommandée.

Solution d'administration et d'exploitation :

- Fournir une solution pour administrer l'ensemble des bornes Wi-Fi de l'établissement.
- Possibilité d'activer les bornes selon des créneaux temporels : jours, heures, ...
- Il est recommandé de pouvoir régler la puissance des bornes en fonction de la surface à couvrir.

Utilisation du Wi-Fi dans le cadre d'un accès de base à Internet :

Le déploiement du Wi-Fi a usage pédagogique est validé par la DSI du vice-rectorat depuis 2013 suivant les directives de la DGESCO-STSI. Notamment, il conviendra de respecter l'ensemble des dispositifs à prévoir dans le cas de la mise en place des « Service numériques et protection des mineurs » : <http://eduscol.education.fr/cid57087/testes-officiels-et-preconisations.html>

Référentiel technique des infra info des lycées

Il s'agira notamment de filtrer les accès à Internet et de conserver pendant 1 an les traces des usagers. (cf. **Annexe 7**).

Le Wi-Fi a été installé :

- Au lycée Jules Garnier
- Au lycée du Grand Nouméa
- Au lycée Escoffier
- Au lycée de Augustin Ty (Touho)
- Au lycée du Mont-Dore

La mise à disposition d'une borne Wi-Fi permettant un usage de base à Internet **doit être un complément** du câblage filaire. Elle apportera une plus grande souplesse et liberté d'utilisation pour les usages peu gourmands en débit (navigation web, portail ENT, ...).

La mise en place d'un tel accès doit respecter les directives de la circulaire du 18 Mai 2006 et sera validée par la DSI et le RSSI du vice-rectorat.

Une solution a été testée et validée par la DSI.

Utilisation du Wi-Fi dans le cadre d'un accès au réseau administratif :

Cette utilisation est strictement interdite et non prévue à ce jour.

Utilisation du Wi-Fi infrastructure dans le cadre d'un accès au réseau pédagogique (Wi-Fi privé) :

La mise à disposition d'une borne Wi-Fi permettant l'usage d'Internet et l'accès aux ressources du serveur pédagogique (Scribe) est autorisé principalement pour les solutions mobiles appartenant à l'établissement (tablettes, ordinateurs portables, ...)

Une solution a été testée et validée par la DSI.

Utilisation du Wi-Fi nomade dans le cadre d'un accès au réseau pédagogique (Wi-Fi privé) :

A défaut d'infrastructure Wi-Fi dans l'établissement (recommandée), le déploiement de classes mobiles avec des points d'accès Wi-Fi sur le **réseau pédagogique** est **autorisé par la DSI** du vice-rectorat depuis 2013 suivant les directives de la DGESCO-STSI.

H. La segmentation du réseau en Vlan

La refonte de l'architecture informatique des établissements prévoit l'intégration de réseaux locaux virtuels (Vlan).

Les Vlan présentent les intérêts suivants :

- Amélioration de la gestion du réseau ;
- Optimisation de la bande passante ;
- Séparation des flux ;
- Segmentation des domaines de broadcast ;
- Amélioration de la sécurité...

L'intégration de cette technologie doit respecter un ensemble de règles communes. Ce document présente la matrice des Vlan qui devra être en application sur la nouvelle architecture réseau des établissements.

Référentiel technique des infra info des lycées

Matrice des Vlan

Nom du Vlan	Vlan	Couleur	Description
Extérieur	7	Red	Accès Internet (10.10.10.x)
Réseau	10	Light Red	Administration éléments actifs
Dmz	16	Yellow	Dmz publique
Wifipub	26	Purple	Wifi public
Voip	36	Orange	Voix sur IP
Ctrlacc	37	Cyan	Contrôle d'accès
Adminsmb	46	Blue	Réseau administratif établissement
Pedago	56	Light Green	Réseau pédagogique établissement
Wifipriv	56	Purple	Extension réseau pédagogique
Videosurv	60	Olive Green	Vidéo surveillance
Domotique	70	Grey	Réseau domotique

Pour les switches en cascade du réseau :

- « administratif » : l'ensemble des ports devront transporter simultanément les Vlan **46** (adminsmb) et **36** (voip) ;
- « Pédago » : l'ensemble des ports devront transporter simultanément les Vlan **56** (pédago) et **36** (voip).

Exemple de schéma du cœur de réseau pour un switch 24 ports :

Numéro du VLAN	Trunk	Trunk	7	7	46	46	16	36	56				Trunk
Port du Commutateur	1	3	5	7	9	11	13	15	17	19	21	23	25
	ESXi ETH 0	ESXi ETH 2	ADSL		NAS A ETH 0		NAS P ETH 0	A*					FO
	ESXi ETH 1	ESXi ETH 3	Onduleur		NAS A ETH 1		NAS P ETH 1						FO
Port du Commutateur	2	4	6	8	10	12	14	16	18	20	22	24	26
Numéro du VLAN	Trunk	Trunk	7	7	46	46	16	36	56				Trunk
	Agr1 (1-4)				Agr2 (9/10)		Agr3 (13/14)						Agr4 (25-26)

Exemple de schéma du réseau pédagogique pour un switch 24 ports :

Numéro du VLAN	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	Trunk
Port du Commutateur	1	3	5	7	9	11	13	15	17	19	21	23	25
	Pedago												FO
													FO
Port du Commutateur	2	4	6	8	10	12	14	16	18	20	22	24	26
Numéro du VLAN	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	56+36	Trunk
													Agr (25-26)

Tous les ports sont configurés en mode Trunk avec comme Vlan natif le réseau pédagogique **56** et comme autre vlan le réseau voip **36**.

Référentiel technique des infra info des lycées

Exemple de schéma du réseau administratif pour un switch 24 ports :

Numéro du VLAN	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	Trunk
Port du Commutateur	1	3	5	7	9	11	13	15	17	19	21	23	25	
													FO	
													FO	
Port du Commutateur	2	4	6	8	10	12	14	16	18	20	22	24	26	
Numéro du VLAN	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	46+36	Trunk Agr (25-26)	

Tous les ports sont configurés en mode Trunk avec comme Vlan natif le réseau administratif 46 et comme autre vlan le réseau voip 36.

Des listes d'accès seront mises en place selon le tableau du paragraphe suivant :

vlan		7	16	26	36	70	56	56	37	60	46
	De \ Vers	Extérieur	Dmz	Wifipub	Voip	Domo	Pedago	Wifipriv	Ctrlacc	Videosu	Admins
7	Extérieur		Interdit	Interdit	Interdit	Interdit	Interdit	Interdit	Interdit	Interdit	Interdit
16	Dmz	Contrôlé		Interdit	Interdit	Interdit	Contrôlé	Interdit	Interdit	Interdit	Contrôlé
26	Wifipub	Contrôlé	Autorisé		Interdit	Interdit	Interdit	Interdit	Interdit	Interdit	Interdit
36	Voip	Contrôlé	Autorisé	Autorisé		Interdit	Contrôlé	Contrôlé	Interdit	Interdit	Contrôlé
70	Domo	Contrôlé	Autorisé	Autorisé	Autorisé		Contrôlé	Interdit	Interdit	Interdit	Interdit
56	Pedago	Contrôlé	Autorisé	Autorisé	Autorisé	Autorisé		Interdit	Interdit	Interdit	Interdit
56	Wifipriv	Contrôlé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé		Interdit	Interdit	Interdit
37	Ctrlacc	Contrôlé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé		Interdit	Contrôlé
60	Videosu	Contrôlé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé		Interdit
46	Admins	Contrôlé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	Autorisé	

Autorisé : Tous les flux sont autorisés par défaut.

Contrôlé : Certains flux sont prédéfinis ou autorisés après demande et validation de la DSI

Interdit : Tous les flux sont interdits

I. Les tablettes

La DSI recommande l'usage de tablettes du système d'exploitation Android pour faciliter l'interopérabilité avec les solutions actuellement déployées au sein des établissements.

La DANE propose un guide pratique pour l'intégration des tablettes sous Android.

J. La vidéosurveillance

L'usage de la vidéo protection est régi par l'article 10 de la loi n° 95-73 du 21 janvier 1995 modifiée et par son décret d'application n° 96-926 du 17 octobre 1996 modifié. Ainsi, la dite loi détermine les lieux dans lesquels un dispositif de vidéo protection peut être installé ; **notamment l'intérieur des lieux et établissements ouvert au public.**

Par ailleurs, une demande d'autorisation doit être formulée auprès du Haut-commissaire.

Référentiel technique des infra info des lycées

L'installation d'un système de vidéo protection sans autorisation est passible de 3 ans d'emprisonnement et de 5 369 928 F CFP d'amende.

Vous trouverez en **Annexe 5** la documentation « vidéosurveillance » et le formulaire de demande d'autorisation « CERFA n° 13806*01 ». D'autres documents seront à fournir avec ce formulaire (détaillé dans la documentation).

Enfin, vous trouverez également en **Annexe 6** une documentation détaillée de la CNIL sur la vidéosurveillance dans les établissements scolaires. Une déclaration à la CNIL devra également être réalisée.

K. Les serveurs

Les serveur doivent être accompagnés **d'une garantie de 3 ans avec une intervention sur site sous 4 heures ouvrables (hors délais de route)** en cas de panne matérielle.

L'infrastructure cible pour les lycées publics comporte deux serveurs physiques (permettant ainsi une répartition de charge et un plan de reprise en mode dégradé) qui composent le serveur virtuel ESX contenant les serveurs (firewalls, administratif, pédagogique, Pronote, ...).

L'hyperviseur vSphere (ESX) est un produit proposé par VMware. Il est entièrement fonctionnel et permet de virtualiser des serveurs et d'exécuter des applications sur des machines virtuelles.

L. L'espace de sauvegarde

Il s'agit de proposer pour un établissement une solution de sauvegarde sur NAS :

- Un NAS pour le réseau administratif. Dans ce cas, seul le serveur « Horus » pourra envoyer des sauvegardes sur ce NAS. Aucune connexions de postes de travail sont autorisées.
- Un NAS pour le réseau DMZ. Dans ce cas, seul le serveur « Scribe » pourra envoyer des sauvegardes sur ce NAS. Aucune connexions de postes de travail sont autorisées.

M. Les services

Il convient de distinguer les services offerts sur le réseau et les serveurs associés en 4 grandes catégories :

- **Catégorie 1** : Les serveurs indispensables au fonctionnement de l'établissement et à son intégration au système d'information du vice-rectorat. Leur configuration sera effectuée par la DSI
- **Catégorie 2** : Les serveurs utiles préconisés par la DSI qui apportera un support technique. L'établissement pouvant effectuer un autre choix (sans support technique de la DSI).
- **Catégorie 3** : Les serveurs proposées et préconisés par la DSI avec un contrat de maintenance par un prestataire externe.
- **Catégorie 4** : Les serveurs laissés à l'initiative de l'établissement.

La DSI s'engage à assurer le suivi technique et d'évolution des serveurs des catégories 1, 2 et 3, ainsi que l'assistance et les formations associées.

Pour des raisons de cohérence et de compatibilité, **l'ensemble des serveurs devra faire l'objet d'une validation technique préalable auprès de la DSI**. Les serveurs physiques de catégorie 1, 2 et 3 devront également être livrés à la DSI avant leurs implantations en établissement pour y être configurés.

Dans le cadre de la virtualisation des serveurs d'applications, la demande de créer des machines virtuelles doit être faite auprès de la DSI par le Chef d'établissement, pour une implémentation sur le serveur physique.

La maintenance des matériels est assurée par un marché public pour les Lycées.

Les services administratifs :

- Horus (serveur virtuel administratif) _____ catégorie 1
- Pronote Serveur (serveur virtuel administratif) _____ catégorie 4

Les services pédagogiques :

- Scribe (serveur virtuel pédagogique, Envole) _____ catégorie 2

Référentiel technique des infra info des lycées

- BCDI (serveur virtuel pédagogique) _____ catégorie 4

Les services téléphoniques pour les lycées :

- XIVO (serveur virtuel téléphonique) _____ catégorie 3

Les services communs :

- WSUS (serveur virtuel de mise à jour, Anti-virus, pronote relais) _____ catégorie 2
- Pfsense (serveur virtuel Wi-Fi) _____ catégorie 2

Les services de sauvegardes :

- NAS _____ catégorie 2

Pare-feu :

- Amon (serveur virtuel pare-feu) _____ catégorie 1

Détail des services offerts par les serveurs :

- Fédération et sécurisation des réseau administratifs et pédagogiques, un seul abonnement Internet **Amon**
- Gratuité des services **Amon/Horus/Scribe/Xivo/Pfsense**
- Applications Nationales en réseau (GFC, GFE) **Horus**
- Répertoires personnels sur le réseau avec possibilités de créer des répertoires d'échanges depuis les réseaux administratifs et pédagogique **Horus/Scribe**
- Télémaintenance des serveurs à distance **Tous**
- Interfaces d'administration via le web simplifiée pour l'administrateur local **Tous**
- Authentification des utilisateurs et gestion des droits par annuaire LDAP pour le réseau administratif **Horus**
- Authentification des utilisateurs et gestion des droits par annuaire LDAP pour le réseau pédagogique avec extraction Sconet, traçage des connexions et réplication **Scribe**
- Sauvegardes automatisées **Horus/Scribe/Machines virtuelles**
- Mise à jour du système des serveurs via le réseau **Tous**

Référentiel technique des infra info des lycées

N. Les périmètres de responsabilités

Les périmètres de responsabilité de l'infrastructure d'un lycée :

Thème	Situation actuelle	Réseau administratif	Réseau pédagogique
Télécom.	Liaison FAI (Lagoon par convention)	Etablissement	
	Acquisition routeur Internet sans Wi-Fi	DSI – VR	
	Installation routeur Internet sans Wi-Fi		
	Raccordement VR-Etablissement via réseau agriates	DSI – VR	
Câblage : FO + cuivre	Préconisation	DSI – VR	
	Installation	Etablissement	
	Maintenance		
Téléphonie	Préconisation : IPBX	DSI – VR	
	Installation	Prestataire	
	Maintenance		
Wi-Fi	Préconisation	Interdit	DSI – VR
	Installation		
	Maintenance		
Commutateur	Préconisation	DSI – VR	
	Installation	Prestataire du marché	
	Maintenance		
Serveurs	Préconisation	DSI – VR	
	Acquisition		
	Installation		
	Maintenance Niv. 1 – Matériel	Prestataire du marché	
	Maintenance Niv. 2 – Système	DSI – VR	
	Maintenance Niv. 3 – Logiciels		
Postes de travail	Préconisation postes de travail	DSI – VR	DANE
	Acquisition	Etablissement	
	Installation		
	Maintenance Niv. 1 – Matériel		
	Maintenance Niv. 2 – Système		
	Maintenance Niv. 3 – Logiciels standard		
	Maintenance Niv. 3 – Logiciels acquis par l'établissement		
	Maintenance Niv. 3 – Applications nationales (GFC, Presto, Sagesse)	DSI – VR	

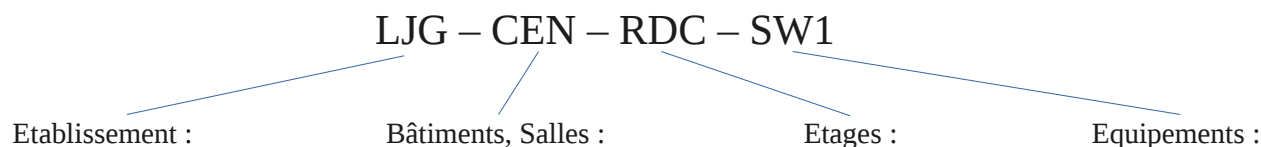
Référentiel technique des infra info des lycées

Thème	<u>CIBLE</u>	Réseau administratif	Réseau pédagogique
Télécom.	Liaison FAI (Lagoon par convention)	Etablissement	
	Acquisition routeur Internet sans Wi-Fi	DSI – VR	
	Installation routeur Internet sans Wi-Fi		
	Raccordement VR-Etablissement via réseaux agriates		
Câblage : FO + cuivre	Préconisation	DSI – VR	
	Installation	Prestataire du marché	
	Maintenance	Etablissement / Prestataire	
Téléphonie	Préconisation : IPBX	DSI – VR	
	Installation	Prestataire / DSI – VR	
	Maintenance	Prestataire /Etablissement / DSI	
Wi-Fi	Préconisation	Interdit	DSI – VR
	Installation		Prestataire marché
	Maintenance		Etab. / DSI
Commutateur	Préconisation	DSI – VR	
	Installation	Prestataire du marché	
	Maintenance2048	Etablissement / Prestataire / DSI	
Serveurs	Préconisation	DSI – VR	
	Acquisition		
	Installation		
	Maintenance Niv. 1 – Matériel	Prestataire du marché	
	Maintenance Niv. 2 – Système	DSI – VR	
	Maintenance Niv. 3 – Logiciels		
Postes de travail	Préconisation postes de travail	DSI – VR	DANE
	Appel d’Offre (marché ou groupement d’achat)	DSI – VR / AGCPT	
	Acquisition	Etablissement / DSI – VR	
	Installation	Prestataire	
	Maintenance Niv. 1 – Matériel		
	Maintenance Niv. 2 – Système		
	Maintenance Niv. 3 – Logiciels standard	Etablissement	
	Maintenance Niv. 3 – Logiciels acquis par l’établissement		
	Maintenance Niv. 3 – Applications nationales (GFC, Presto, Sagesse)	DSI – VR	

Référentiel technique des infra info des lycées

O. Nommage des équipements

Le nommage des éléments actifs ou périphériques a une importance. Il permet de localiser l'équipement et sert de référence dans l'inventaire de l'établissement. Il sera établi sous la forme suivante :



Attiti	ATT
Haudra	HAU
Kela	KLA
Laperouse	LAP
Lgn	LGN
Lpch	LPCH
Garnier	LJG
Touho	TOU
Montdore	LMD
Alp-koumac	ALP-KMC
Alp-Lafoa	ALP-LAFOA
Alp-laroche	ALP-LAROCHE

Salle serveur	CEN
Bâtiment	BAT1
CDI	CDI
Réfectoire	CAN
Internat	INT
Logement	LOG
Infirmirmerie	INF
EPS	EPS

Rez-chaussé	RDC
Etage 1	E1
Etage 2	E2
Etage 3	E3
Sous-sol	SSL

Switch	SW
Borne	BRN
Tel. IP	TEL
Routeur ADSL	ADSL
Routeur FO	FO
Imprimante	IMP
Fax	FAX
Client Lég.	LEG
Caméra	CAM

III. L'espace numérique de travail (ENT)

Un ENT a été déployé sur l'ensemble des lycées publics de la Nouvelle-Calédonie (socle ENVOLE).

Les établissements bénéficieront du support technique de la DSI.

Prévoir un comité de pilotage ENT et un référent ENT pédagogique par établissement (des formations sont prévues par la DANE).