

LELOUP Quentin  
LECOQ Enguerran

Rapport SAE 33



## Sommaire

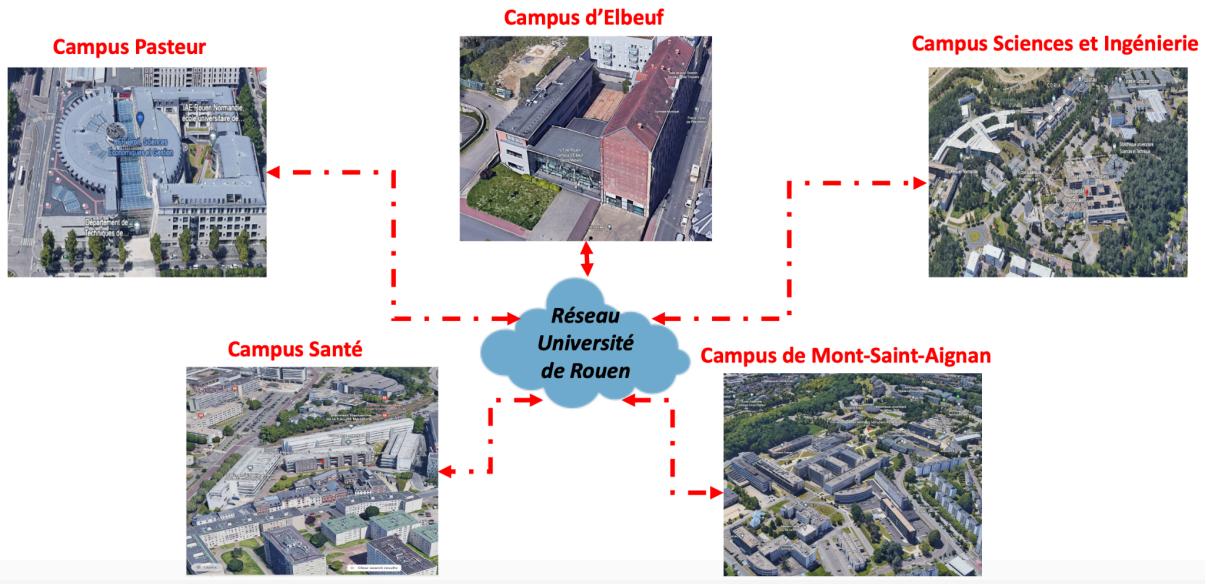
<b>1. Problématique :</b>	<b>4</b>
Convention de nommage :	4
<b>2. Solution adoptée :</b>	<b>5</b>
Schéma infrastructure :	5
Explication :	6
Baies infrastructure :	7
Tableau VLAN / IP : Segmentation IP/VLAN	9
Cisco Packet Tracer :	10
<b>1. Sécurité et fonctionnalités :</b>	<b>11</b>
DHCP :	11
HSRP :	11
Protocole de routage :	11
Firewall :	13
ACL	13
QoS	13
Chiffrement & IPSEC :	15
Sécurisation d'accès aux équipements :	16
Mot de passe :	16
Serveur TACACS :	16
Wi-Fi :	17
SNMP	17
<b>4. Chiffrage :</b>	<b>18</b>
CHOIX DU MATERIEL :	18
CÂBLAGE :	18
ROCADE FIBRE :	19
SWITCH :	19
ONDULEUR :	20
ROUTEUR 4G :	21
ROUTEUR :	21
TRANSCEIVER FIBRE/RJ45 (SI BESOIN) :	22
MODULE SFP :	22
FIREWALL :	23
SERVEUR :	23
BAIE :	24
TOTAL :	25
Baie cœur de réseau :	25
Baie autres sites :	25
<b>5. Proposition d'évolution :</b>	<b>26</b>
MPLS :	26
PPPOE:	26
AD :	26
Formation des utilisateurs :	26

<b>6. Glossaire.....</b>	<b>27</b>
DHCP :.....	27
OSPF :.....	27
ACL :.....	27
QoS :.....	27
Tunnel IPSEC :.....	27
SSH.....	27
TACACS+.....	28
SNMP.....	28
WPA2-PSK.....	28
HSRP :.....	28

# 1. Problématique :

Nous devons créer une infrastructure réseau complète et sécurisée pour l'université de Rouen, nous devons réaliser une liaison multisite.

Cette liaison doit suivre le modèle suivant :



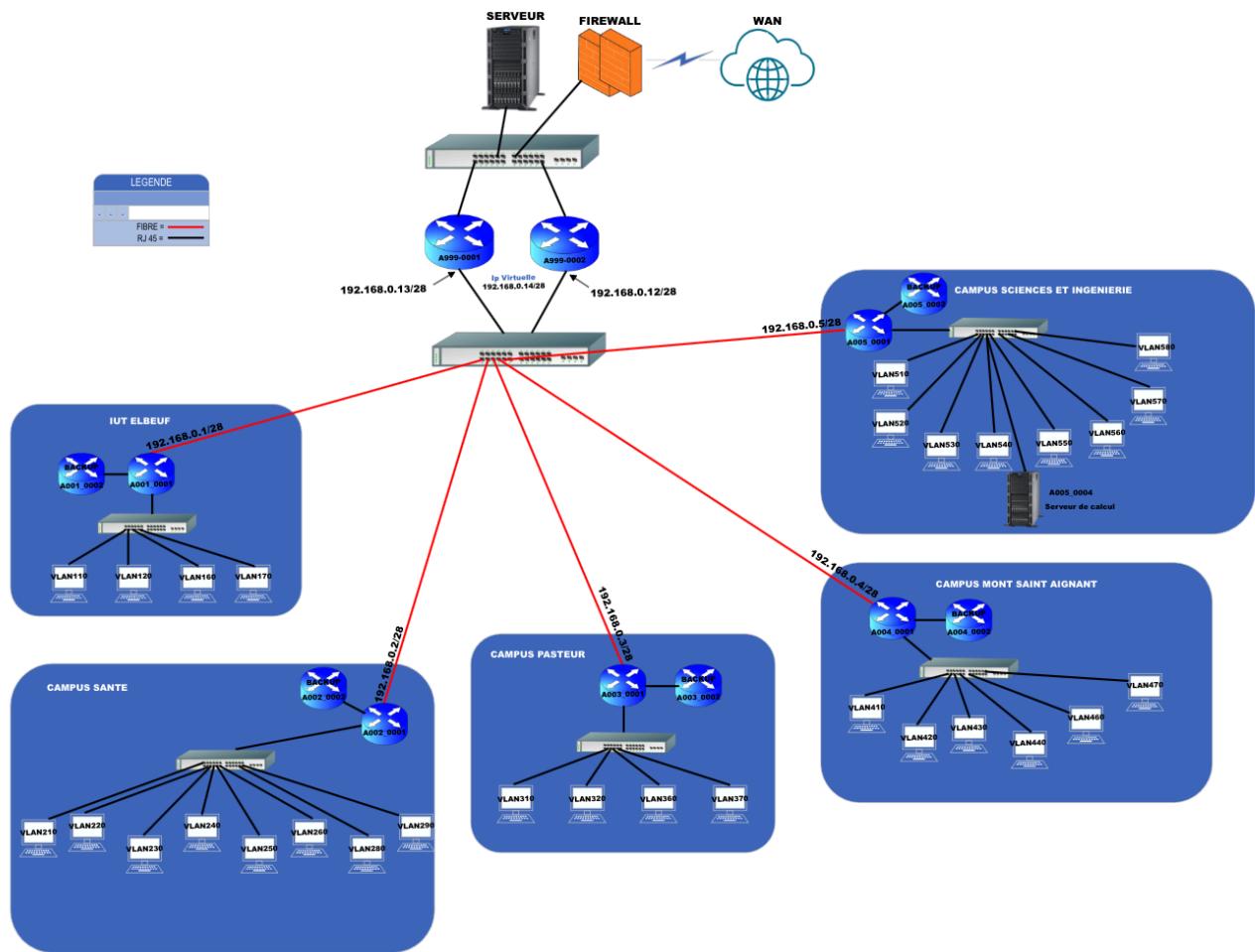
On peut voir sur le schéma ci-dessus que les 5 sites doivent pouvoir communiquer. Nous avons opté pour une infrastructure opérateur, ou un PoP est présent qui permet de sortir sur internet. C'est pourquoi chaque site est relié au PoP par une FON (Fibre Optique Noir) et chaque site possède un routeur 4G de backup.

## Convention de nommage :

Nous proposons la convention de nommage des équipements suivante : A<ref site en nombre>\_<ref équipement en nombre>. Nous proposons que le cœur de réseau soit le dernier site possible, donc A999. La lettre pourra également être changée si le besoin y est. Grâce à cette convention, nous pouvons avoir 25974 sites et 999 équipements réseau/site

## 2.Solution adoptée

Schéma infrastructure :



Pour agrandir l'image > [INFRA\\_GLOBALE.png](#)

Nous avons choisi une topologie de réseau de ce type car pour nous il est important de conserver une infrastructure de type opérateur afin de pouvoir dépanner plus facilement.

## Explication :

Le cœur de réseau se trouve dans un bâtiment PoP (Point of Presence) à l'extérieur des universités.

Ce choix a été fait pour rendre le réseau facilement administrable et pour isoler les équipements par fonctionnalité.

Dans ce bâtiment se trouve : Les 2 routeurs principaux, un firewall et un serveur central.

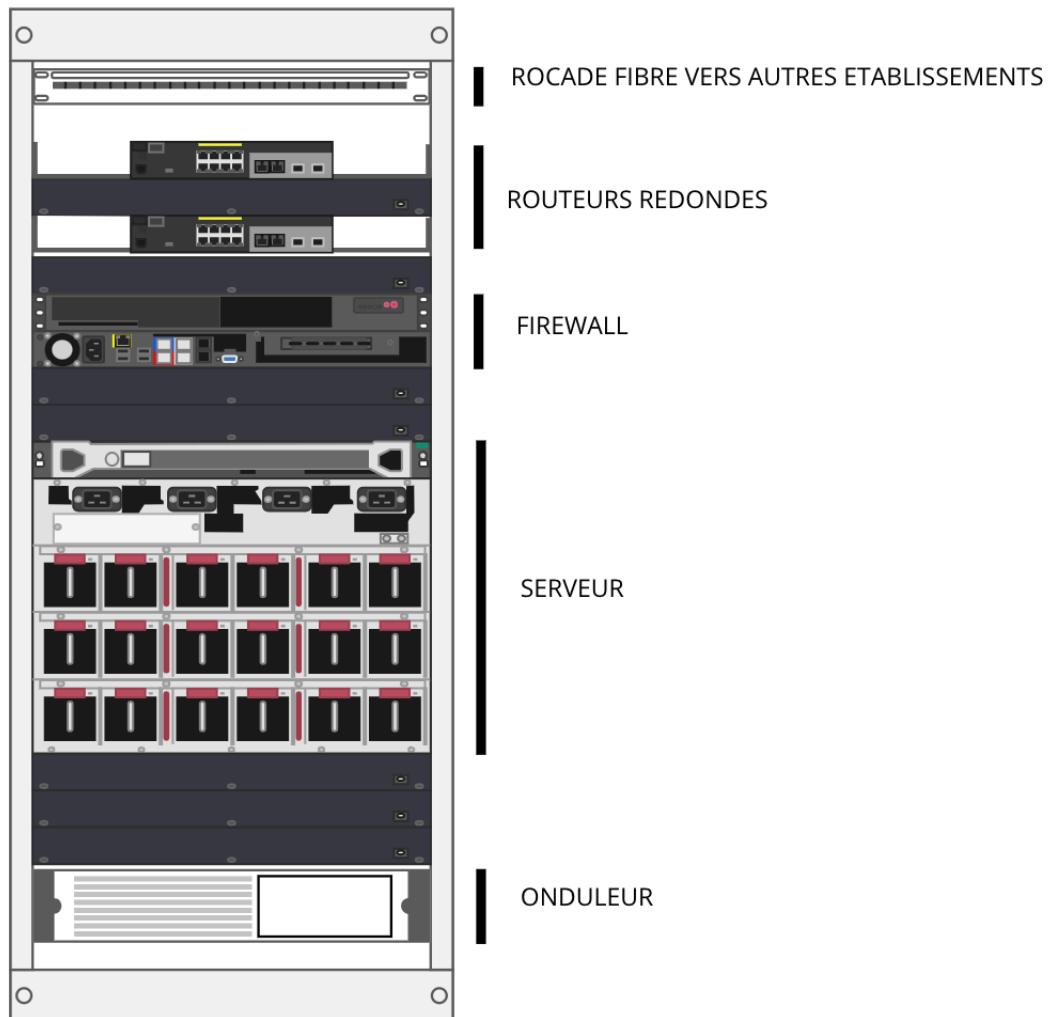
Des fibres noires dédiées partent de ce bâtiment pour desservir chaque site.

Chaque site possède deux routeurs dont un dédié au Backup 4G.

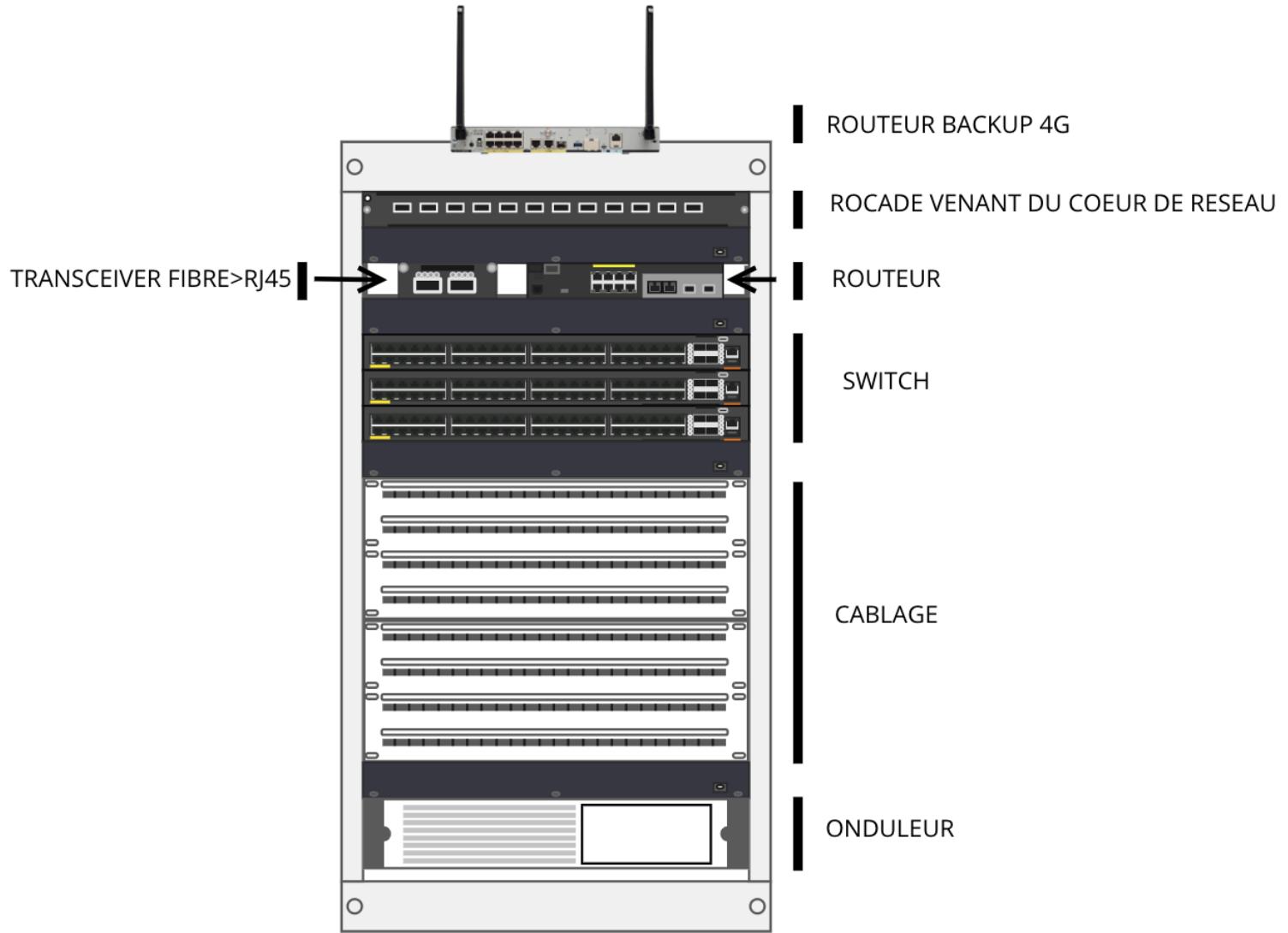
Les différentes formations et services des écoles sont associés à un VLAN unique.

Baies infrastructure :

## BAIE COEUR DE RESEAU



## BAIE DES DIFFERENTES UNITEES



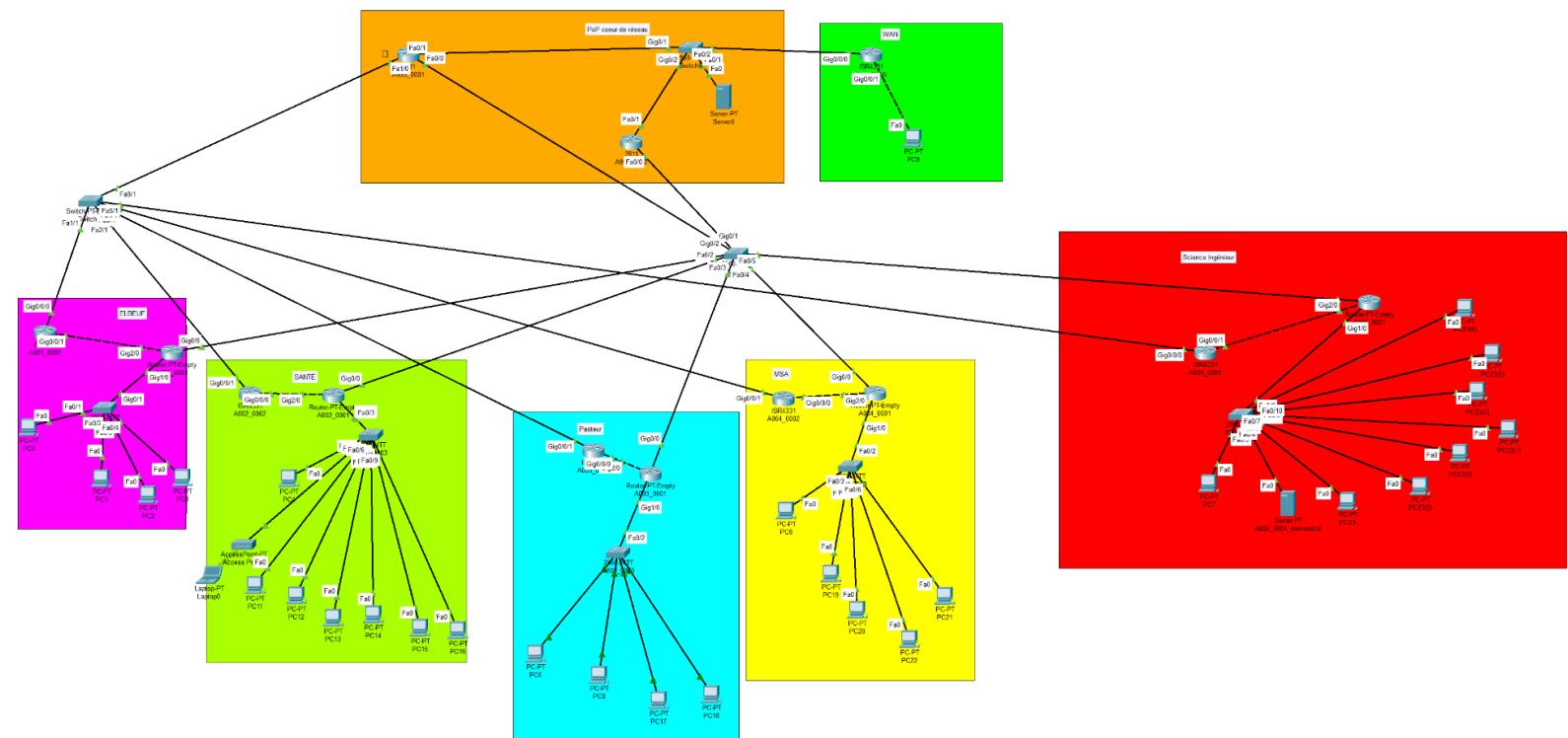
Pour apporter une sécurité supplémentaire en termes de panne, dans chaque baie il y aura un onduleur qui permettra d'alimenter la baie pendant environ 1H s'il y a une coupure de courant.

## Tableau VLAN / IP : Segmentation IP/VLAN

ETABLISSEMENT -- routeur	INTERFACE	@IP	VLAN ID	NAME	MASK	RANGE
A001_0001	Gi1/0	10.1.11.254	110	RT	/23	10.1.10.1 > 10.1.11.254
A001_0001	Gi1/0	10.1.21.254	120	MMI	/23	10.1.20.1 > 10.1.21.254
A001_0001	Gi1/0	10.1.60.254	160	PROFS	/24	10.1.60.1 > 10.1.60.254
A001_0001	Gi1/0	10.1.70.254	170	ADM/TECH	/24	10.1.70.1 > 10.1.70.254
A001_0001	Gi0/0	192.168.0.1	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A001_0001	Gi2/0	172.0.0.2	x	INTERCO BACKUP	/30	172.0.0.1 > 172.0.0.2
A001_0002	Gi0/0/1	172.0.0.1	x	INTERCO BACKUP	/30	172.0.0.1 > 172.0.0.2
A001_0002	Gi0/0/0	1.1.1.1	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A001_0001	Lo0	198.18.0.1	x	Loopback SUP	/30	198.18.0.1 > 198.18.0.2
A001_0002	Lo0	198.18.0.2	x	Loopback SUP	/30	198.18.0.1 > 198.18.0.2
A002_0001	Gi1/0	10.2.15.254	210	MEDECINE	/21	10.2.8.1 > 10.2.15.254
A002_0001	Gi1/0	10.2.23.254	220	PHARMA	/21	10.2.16.1 > 10.2.23.254
A002_0001	Gi1/0	10.2.39.254	230	ODONTHOLOGIE	/21	10.2.32.1 > 10.2.39.254
A002_0001	Gi1/0	10.2.47.254	240	ORTOPHONIE	/21	10.2.40.1 > 10.2.47.254
A002_0001	Gi1/0	10.2.55.254	250	PARAMEDICAL	/21	10.2.48.1 > 10.2.55.254
A002_0001	Gi1/0	10.2.61.254	260	PROFS	/23	10.2.60.1 > 10.2.61.254
A002_0001	Gi1/0	10.2.80.254	280	INGE	/24	10.2.80.1 > 10.2.80.254
A002_0001	Gi1/0	10.2.90.254	290	DOCTEUR	/24	10.2.90.1 > 10.2.90.254
A002_0001	Gi0/0	192.168.0.2	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A002_0001	Gi2/0	172.0.0.6	x	INTERCO BACKUP	/30	172.0.0.5 > 172.0.0.6
A002_0002	Gi0/0/0	172.0.0.5	x	INTERCO BACKUP	/30	172.0.0.5 > 172.0.0.6
A002_0002	Gi0/0/1	1.1.1.2	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A002_0001	Lo0	198.18.0.5	x	Loopback SUP	/30	198.18.0.5 > 198.18.0.6
A002_0002	Lo0	198.18.0.6	x	Loopback SUP	/30	198.18.0.5 > 198.18.0.6
A003_0001	Gi1/0	10.3.15.254	310	UFR DROIT	/21	10.3.8.1 > 10.3.15.254
A003_0001	Gi1/0	10.3.23.254	320	IUT ROUEN	/21	10.3.16.1 > 10.3.23.254
A003_0001	Gi1/0	10.3.63.254	360	PROFS	/22	10.3.60.1 > 10.3.63.254
A003_0001	Gi1/0	10.3.70.254	370	ADM/TECH	/24	10.3.70.1 > 10.3.70.254
A003_0001	Gi0/0	192.168.0.3	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A003_0001	Gi2/0	172.0.0.10	x	INTERCO BACKUP	/30	172.0.0.9 > 172.0.0.10
A003_0002	Gi0/0/0	172.0.0.9	x	INTERCO BACKUP	/30	172.0.0.9 > 172.0.0.10
A003_0002	Gi0/0/1	1.1.1.3	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A003_0001	Lo0	198.18.0.9	x	Loopback SUP	/30	198.18.0.9 > 198.18.0.10
A003_0002	Lo0	198.18.0.10	x	Loopback SUP	/30	198.18.0.9 > 198.18.0.10
A004_0001	Gi1/0	10.4.15.254	410	IUT ROUEN	/21	10.4.8.1 > 10.4.15.254
A004_0001	Gi1/0	10.4.23.254	420	UFR SCI & TECH	/21	10.4.16.1 > 10.4.23.254
A004_0001	Gi1/0	10.4.39.254	430	UFR LETTRES & SCI HUMAINES	/21	10.4.32.1 > 10.4.39.254
A004_0001	Gi1/0	10.4.47.254	440	UFR SCI DE L'HOMME & SOCIETE	/21	10.4.40.1 > 10.4.47.254
A004_0001	Gi1/0	10.4.63.254	460	PROFS	/22	10.4.60.1 > 10.4.63.254
A004_0001	Gi1/0	10.4.71.254	470	ADM/TECH	/22	10.4.68.1 - 10.4.71.254
A004_0001	Gi0/0	192.168.0.4	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A004_0001	Gi2/0	172.0.0.14	x	INTERCO BACKUP	/30	172.0.0.13 > 172.0.0.14
A004_0002	Gi0/0/0	172.0.0.13	x	INTERCO BACKUP	/30	172.0.0.13 > 172.0.0.14
A004_0002	Gi0/0/1	1.1.1.4	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A004_0001	Lo0	198.18.0.13	x	Loopback SUP	/30	198.18.0.13 > 198.18.0.14
A004_0002	Lo0	198.18.0.14	x	Loopback SUP	/30	198.18.0.13 > 198.18.0.14
A005-0001	Gi1/0	10.5.15.254	510	UFR SCI TECHNIQUE	/21	10.5.8.1 > 10.5.15.254
A005-0001	Gi1/0	10.5.23.254	520	LABO LITIS	/21	10.5.16.1 > 10.5.23.254
A005-0001	Gi1/0	10.5.39.254	530	LABO CORIA	/21	10.5.32.1 > 10.5.39.254
A005-0001	Gi1/0	10.5.47.254	540	LABO LMI	/21	10.5.40.1 > 10.5.47.254
A005-0001	Gi1/0	10.5.55.254	550	CENTRE DE CALCUL	/21	10.5.48.1 > 10.5.55.254
A005-0001	Gi1/0	10.5.63.254	560	PROF	/22	10.5.60.1 > 10.5.63.254
A005-0001	Gi1/0	10.5.71.254	570	ADM/TECH	/23	10.5.70.1 > 10.5.71.254
A005-0001	Gi1/0	10.5.81.254	580	CHERCHEUR	/23	10.5.80.1 > 10.5.81.254
A005-0001	Gi0/0	192.168.0.5	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A005-0001	Gi2/0	172.0.0.18	x	INTERCO BACKUP	/30	172.0.0.17 > 172.0.0.18
A005-0002	Gi0/0/1	172.0.0.17	x	INTERCO BACKUP	/30	172.0.0.17 > 172.0.0.18
A005-0002	Gi0/0/0	1.1.1.5	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A005-0001	Gi0/0/1	198.18.0.17	x	Loopback SUP	/30	198.18.0.17 > 198.18.0.18
A005-0002	Gi0/0/1	198.18.0.18	x	Loopback SUP	/30	198.18.0.17 > 198.18.0.18
A999_0001	Fa0/0	192.168.0.13	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A999_0002	Fa0/0	192.168.0.12	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A999_000(virtuelle)	Fa0/0	192.168.0.14	x	INTERCO COEUR DE RESEAU	/28	192.168.0.1 > 192.168.0.14
A999_0001	Fa0/1	192.168.10.253	x	DMZ	/24	192.168.10.1 > 192.168.10.254

A999_0002	Fa0/1	192.168.10.252	x	DMZ	/24	192.168.10.1 > 192.168.10.254
A999_000(virtuelle)	Fa0/1	192.168.10.254	x	DMZ	/24	192.168.10.1 > 192.168.10.254
A999_0001	Fa1/0	1.1.1.14	x	TUNNEL IPSEC	/28	1.1.1.1 > 1.1.1.14
A999_0001	Lo0	198.18.0.21	x	Loopback SUP	/30	198.18.0.21 > 198.18.0.22
A999_0002	Lo0	198.18.0.22	x	Loopback SUP	/30	198.18.0.21 > 198.18.0.22
A999_0003	gi0/0/0	192.168.10.100	x	WAN	/8	8.0.0.0 > 8.255.255.254
A999_0003	gi0/0/1	8.8.8.8	x	DMZ	/24	198.18.0.21 > 198.18.0.22

## Cisco Packet Tracer :



Par soucis avec packet tracer, nous simulons le backup 4G par des routeurs reliés à un switch qui sont connectés au PE (Provider Edge) de collecte IPSEC (A999\_0001) avec des IP publiques.

# 1. Sécurité et fonctionnalités :

## DHCP :

Nous proposons des serveurs DHCP qui sont sur chaque routeur, nous mettons donc en place un pool DHCP pour chaque VLAN, nous mettons comme DNS le DNS interne, cependant nous ne pouvons pas simuler le DNS google (8.8.8.8) alors nous ne l'avons pas renseigné, mais nous conseillons de le mettre en DNS secondaire lors du déploiement.

Template configuration des DHCP :

```
ip dhcp pool VLAN<ID_VLAN>
network <@réseau> <masqueréseau>
default-router <@_routeur>
dns-server 192.168.10.1
```

Concernant les réservation IP, nous pouvons le faire avec l'adresse MAC, voici un exemple pour le site de Science Ingénieur avec le serveur de calcul :

```
ip dhcp excluded-address 192.168.10.253
```

## HSRP :

Nous mettons en place ce protocole pour avoir une redondance des PE de collecte et une résistance à la panne.

Template configuration équipement primaire

```
standby 100 ip <ip virtuelle>
standby 100 priority 110
standby 100 preempt
```

Template configuration équipement secondaire

```
standby 100 ip <ip virtuelle>
standby 100 priority 90
standby preempt
```

## Protocole de routage :

Nous proposons le protocol OSPF (Open Shortest Path First) car nous sommes dans un réseau MAN (Réseau métropolitain) et que ce protocole est adapté à un réseau de cette envergure.

## *Routes ospf sur le PE A999\_0001 :*

```
A999_0001#sh ip route ospf
10.0.0.0/8 is variably subnetted, 35 subnets, 5 masks
O 10.1.10.0 [110/2] via 192.168.0.1, 00:09:00, FastEthernet0/0
O 10.1.20.0 [110/2] via 192.168.0.1, 00:09:00, FastEthernet0/0
O 10.1.60.0 [110/2] via 192.168.0.1, 00:09:00, FastEthernet0/0
O 10.1.70.0 [110/2] via 192.168.0.1, 00:09:00, FastEthernet0/0
O 10.2.8.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.16.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.32.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.40.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.48.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.60.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.80.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.2.90.0 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 10.3.8.0 [110/2] via 192.168.0.3, 00:09:00, FastEthernet0/0
O 10.3.16.0 [110/2] via 192.168.0.3, 00:09:00, FastEthernet0/0
O 10.3.60.0 [110/2] via 192.168.0.3, 00:09:00, FastEthernet0/0
O 10.3.70.0 [110/2] via 192.168.0.3, 00:09:00, FastEthernet0/0
O 10.4.8.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.4.16.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.4.32.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.4.40.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.4.60.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.4.68.0 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 10.5.8.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.16.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.32.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.40.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.48.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.60.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.70.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 10.5.80.0 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
198.18.0.0/24 is variably subnetted, 12 subnets, 2 masks
O 198.18.0.1 [110/2] via 192.168.0.1, 00:09:00, FastEthernet0/0
O 198.18.0.5 [110/2] via 192.168.0.2, 00:09:00, FastEthernet0/0
O 198.18.0.9 [110/2] via 192.168.0.3, 00:09:00, FastEthernet0/0
O 198.18.0.13 [110/2] via 192.168.0.4, 00:09:00, FastEthernet0/0
O 198.18.0.17 [110/2] via 192.168.0.5, 00:09:00, FastEthernet0/0
O 198.18.0.22 [110/2] via 192.168.0.12, 00:09:00, FastEthernet0/0
[110/2] via 192.168.10.252, 00:09:00, FastEthernet0/1
```

Concernant le protocole utilisé pour les CPE 4G, nous avons décidé de mettre en place des routes statiques, la route par défaut vers le PE de collecte IPSEC et une route vers le routeur principal pour joindre le LAN.

Exemple avec le CPE A001\_0002 :

```
A001_0002#sh ip route static
10.0.0.0/16 is subnetted, 1 subnets
S 10.1.0.0 is directly connected, GigabitEthernet0/0/1
[150/0] via 172.0.0.2
S* 0.0.0.0/0 [1/0] via 1.1.1.14
```

## **Firewall :**

Ne pouvant pas simuler un firewall Fortinet sur packet, nous pouvions simuler un firewall Cisco ASA, cependant l'utilisation de celui-ci revient à mettre en place des ACLs et nous permettant pas de mettre en place un VPN pour des utilisateurs à distance, alors nous avons décidé de ne pas le simuler pour ne pas proposer une solution que nous ne validons pas.

## **ACL**

Concernant les ACLs, notre cahier des charges ne nous en imposants aucune, nous proposons uniquement des ACLs étendues qui nous permettent d'autoriser des flux sur la couche 3 & 4 du modèle OSI.

Exemple sur le CPE A005\_0001 où l'on autorise uniquement le ping vers le serveur et des connexions ssh :

```
A005_0001#sh access-lists  
Extended IP access list SSH_calcul  
10 permit icmp any any  
20 permit tcp any 10.5.48.0 0.0.7.255 eq 22
```

Mais également avec le PE de collecte IPSEC où l'on filtre les protocoles :

```
A999_0001#sh access-lists  
Extended IP access list IPSEC  
10 permit ip any any  
20 permit tcp any any  
30 permit udp any any  
40 permit icmp any any
```

Et enfin avec la QoS.

## **QoS**

La QoS nous permet de filtrer les flux et de les prioriser lorsque le lien est saturé. Par souci de possibilités de simulation avec packet tracer, nous ne pouvons appliquer la configuration d'une QoS sur nos PE de collecte Fibre, voici la configuration que nous proposons :

```

class-map match-all A001
match access-group name DATA_A001_0001
class-map match-all A002
match access-group name DATA_A002_0001
class-map match-all A003
match access-group name DATA_A003_0001
class-map match-all A004
match access-group name DATA_A004_0001
class-map match-all A005
match access-group name DATA_A005_0001
policy-map QoS_L2L
class DATA_A001_0001
priority percent 10
class DATA_A002_0001
bandwidth percent 25
class DATA_A003_0001
bandwidth percent 15
class DATA_A004_0001
bandwidth percent 15
class DATA_A005_0001
bandwidth percent 25
policy-map QOS_A999_1G
class class-default
shape average 1000000000 10000000
service-policy QoS_L2L
interface FastEthernet0/0
description *** DISTRI FO ***
no ip redirects
no ip unreachables
no ip proxy-arp
no sh
no cdp enable
service-policy output QOS_A999_1G
ip access-list extended DATA_A001_0001
permit ip 10.1.10.0 0.0.1.255 any
permit tcp 10.1.10.0 0.0.1.255 any
permit udp 10.1.10.0 0.0.1.255 any
permit icmp 10.1.10.0 0.0.1.255 any
permit ip 10.1.20.0 0.0.1.255 any
permit tcp 10.1.20.0 0.0.1.255 any
permit udp 10.1.20.0 0.0.1.255 any
permit icmp 10.1.20.0 0.0.1.255 any
permit ip 10.1.60.0 0.0.0.255 any
permit tcp 10.1.60.0 0.0.0.255 any
permit udp 10.1.60.0 0.0.0.255 any
permit icmp 10.1.60.0 0.0.0.255 any
ip access-list extended DATA_A002_0001
permit ip 10.2.8.0 0.0.7.255 any
permit tcp 10.2.8.0 0.0.7.255 any
permit udp 10.2.8.0 0.0.7.255 any
permit icmp 10.2.8.0 0.0.7.255 any
permit ip 10.2.16.0 0.0.7.255 any
permit tcp 10.2.16.0 0.0.7.255 any
permit udp 10.2.16.0 0.0.7.255 any
permit icmp 10.2.16.0 0.0.7.255 any
permit ip 10.2.32.0 0.0.7.255 any
permit tcp 10.2.32.0 0.0.7.255 any
permit udp 10.2.32.0 0.0.7.255 any
permit icmp 10.2.32.0 0.0.7.255 any
permit ip 10.2.40.0 0.0.7.255 any
permit tcp 10.2.40.0 0.0.7.255 any
permit udp 10.2.40.0 0.0.7.255 any
permit icmp 10.2.40.0 0.0.7.255 any
permit ip 10.2.48.0 0.0.7.255 any
permit tcp 10.2.48.0 0.0.7.255 any
permit udp 10.2.48.0 0.0.7.255 any
permit icmp 10.2.48.0 0.0.7.255 any
permit ip 10.2.60.0 0.0.1.255 any
permit tcp 10.2.60.0 0.0.1.255 any
permit udp 10.2.60.0 0.0.1.255 any
permit icmp 10.2.60.0 0.0.1.255 any
ip access-list extended DATA_A003_0001
permit ip 10.3.8.0 0.0.7.255 any
permit tcp 10.3.8.0 0.0.7.255 any
permit udp 10.3.8.0 0.0.7.255 any
permit icmp 10.3.8.0 0.0.7.255 any
permit ip 10.3.16.0 0.0.7.255 any
permit tcp 10.3.16.0 0.0.7.255 any
permit udp 10.3.16.0 0.0.7.255 any
permit icmp 10.3.16.0 0.0.7.255 any
permit ip 10.3.60.0 0.0.3.255 any
permit tcp 10.3.60.0 0.0.3.255 any
permit udp 10.3.60.0 0.0.3.255 any
permit icmp 10.3.60.0 0.0.3.255 any
ip access-list extended DATA_A004_0001
permit ip 10.4.8.0 0.0.7.255 any
permit tcp 10.4.8.0 0.0.7.255 any
permit udp 10.4.8.0 0.0.7.255 any
permit icmp 10.4.8.0 0.0.7.255 any
permit ip 10.4.16.0 0.0.7.255 any
permit tcp 10.4.16.0 0.0.7.255 any
permit udp 10.4.16.0 0.0.7.255 any
permit icmp 10.4.16.0 0.0.7.255 any
permit ip 10.4.32.0 0.0.7.255 any
permit tcp 10.4.32.0 0.0.7.255 any
permit udp 10.4.32.0 0.0.7.255 any
permit icmp 10.4.32.0 0.0.7.255 any
permit ip 10.4.40.0 0.0.7.255 any
permit tcp 10.4.40.0 0.0.7.255 any
permit udp 10.4.40.0 0.0.7.255 any
permit icmp 10.4.40.0 0.0.7.255 any
permit ip 10.4.60.0 0.0.3.255 any
permit tcp 10.4.60.0 0.0.3.255 any
permit udp 10.4.60.0 0.0.3.255 any
permit icmp 10.4.60.0 0.0.3.255 any
ip access-list extended DATA_A005_0001
permit ip 10.5.8.0 0.0.7.255 any
permit tcp 10.5.8.0 0.0.7.255 any
permit udp 10.5.8.0 0.0.7.255 any
permit icmp 10.5.8.0 0.0.7.255 any
permit ip 10.5.16.0 0.0.7.255 any
permit tcp 10.5.16.0 0.0.7.255 any
permit udp 10.5.16.0 0.0.7.255 any
permit icmp 10.5.16.0 0.0.7.255 any
permit ip 10.5.32.0 0.0.7.255 any
permit tcp 10.5.32.0 0.0.7.255 any
permit udp 10.5.32.0 0.0.7.255 any
permit icmp 10.5.32.0 0.0.7.255 any
permit ip 10.5.40.0 0.0.7.255 any
permit tcp 10.5.40.0 0.0.7.255 any
permit udp 10.5.40.0 0.0.7.255 any
permit icmp 10.5.40.0 0.0.7.255 any
permit ip 10.5.48.0 0.0.7.255 any
permit tcp 10.5.48.0 0.0.7.255 any
permit udp 10.5.48.0 0.0.7.255 any
permit icmp 10.5.48.0 0.0.7.255 any
permit ip 10.5.60.0 0.0.3.255 any
permit tcp 10.5.60.0 0.0.3.255 any
permit udp 10.5.60.0 0.0.3.255 any
permit icmp 10.5.60.0 0.0.3.255 any

```

## Chiffrement & IPSEC :

Nous chiffrons les connexions au routeur en autorisant uniquement des connexions ssh aux routeurs :

```
line vty 0 4
transport input ssh
```

Afin que nos liaisons 4G soient sécurisées nous proposons de mettre en place des tunnels IPSEC, voici les templates de configuration.

template CPE :

```
crypto isakmp policy 100
hash md5
authentication pre-share
!
crypto isakmp key ipsec<Ref_Site_CPE> address <IP_PE_IPSEC>
!
crypto ipsec transform-set TEST esp-aes 128 esp-md5-hmac
!
crypto map MONMAP 10 ipsec-isakmp
set peer <IP_PE_IPSEC>
set transform-set TEST
match address IPSEC
!
interface <Interface_Wan>
crypto map MONMAP
!
in
!
ip access-list extended IPSEC
permit ip any any
permit tcp any any
permit udp any any
permit icmp any any
```

template PE collecte :

```
crypto isakmp policy 100
hash md5
authentication pre-share
!
crypto isakmp key ipsec<Ref_Site_CPE> address <IP_CPE_IPSEC>
!
crypto ipsec transform-set TEST esp-aes 128 esp-md5-hmac
!
crypto map principal 10 ipsec-isakmp
set peer <IP_CPE_IPSEC>
set transform-set TEST
match address IPSEC
!
interface <Interface_Wan>
crypto map principal
ip access-list extended IPSEC
permit ip any any
permit tcp any any
permit udp any any
```

Ainsi nos tunnels IPSEC sont chiffrés avec cette commande :

```
crypto ipsec transform-set TEST esp-aes 128 esp-md5-hmac
```

Cependant, le tunnel est UP seulement quand du flux le traverse.

Par soucis de simulation avec packet tracer, nous ne pouvons créer des requêtes infini pour maintenir les tunnels IPSEC UP. Voici la proposition de configuration :

```
ip sla 20
icmp-echo 1.1.1.14 source-interface <interface_WAN>
frequency 5
ip sla schedule 20 life forever start-time now
```

# Sécurisation d'accès aux équipements :

## Mot de passe :

Pour l'accès à chaque équipement, nous avons mis un mot de passe pour passer en mode 'enable'. Le mot de passe est générique : rancid

Nous conseillons de mettre un mot de passe plus sécurisé et différent par équipement

## Serveur TACACS :

Ce serveur permet de faire une authentification avant de pouvoir accéder aux équipements à distance. Pour faciliter les connexions, les credentials sont : ID -> rancid; password -> rancid. Mais lors du déploiement, nous préconisons d'avoir un ID et mot de passe par employé apte à se connecter aux équipements.

```
A999_0001#  
A999_0001#ssh -l rancid 192.168.0.1  
  
Password:  
A001_0001>  
A001_0001>
```

Template pour activer les authentifications TACACS sur les équipements cisco :

```
enable password rancid  
aaa new-model  
aaa authentication login tacacs group tacacs+ local  
aaa authorization exec default group tacacs+ local  
username rancid password 0 rancid  
tacacs-server host 192.168.10.1 key aze  
line vty 0 4  
login authentication tacacs
```

AAA

Client Name	Client IP	Server Type	Key
1 A999_0001	192.168.0.1	Tacacs	aze
2 A999_0001	192.168.0.2	Tacacs	aze
3 A999_0001	192.168.0.3	Tacacs	aze
4 A999_0001	192.168.0.4	Tacacs	aze
5 A999_0001	192.168.0.5	Tacacs	aze

Network Configuration

Client Name	Client IP	Server Type	Key
1 A999_0001	192.168.0.1	Tacacs	aze
2 A999_0001	192.168.0.2	Tacacs	aze
3 A999_0001	192.168.0.3	Tacacs	aze
4 A999_0001	192.168.0.4	Tacacs	aze
5 A999_0001	192.168.0.5	Tacacs	aze

User Setup

Username	Password
1 rancid	rancid

AAA

Service	Radius Port
<input checked="" type="radio"/> On <input type="radio"/> Off	1645

## Wi-Fi :

Concernant les connexions Wi-Fi, ne pouvant simuler un AD sur packet tracer, nous ne pouvons pas proposer une connexion avec des credentials relier à celui-ci, voici notre proposition pour la simulation :

Port Status	<input checked="" type="checkbox"/> On
SSID	test
2.4 GHz Channel	11
Coverage Range (meters)	140,00
Authentication	
<input type="radio"/> Disabled	<input type="radio"/> WEP
<input checked="" type="radio"/> WPA-PSK	<input checked="" type="radio"/> WPA2-PSK
WEP Key	
PSK Pass Phrase	azertyui
User ID	
Password	
Encryption Type	AES

Ici, nous avons le protocole WPA2-PSK, afin que la connexion soit facilitée, nous avons mis un mot de passe simple, nous préconisons un mot de passe plus sécurisé lors du déploiement.

Par souci de temps, nous avons simulé une seule connexion Wi-Fi pour montrer notre capacité à créer des connexions Wi-Fi

## SNMP

Afin de pouvoir superviser/diagnostiquer les liens/routeurs, nous avons mis en place le protocole SNMP avec la communauté 'getsnmp' en read only.

Configuration mise en place sur les routeurs :

```
snmp-server community getsnmp RO
```

## 4. Chiffrage :

Afin de simplifier la schématisation de notre infrastructure, nous partons du principe qu'il y aura une baie par site. Bien évidemment, si elle est mise en place, il y aura plusieurs sous-baies par site. Nous n'allons pas non plus chiffrer les câbles de brassage et les fibres.

### CHOIX DU MATERIEL :

#### CÂBLAGE :

Bandeau 48p Cat6 3M > **150e pièce**



Avec noyaux RJ45  
3M/CORNING  
Bindés en Cat6 >  
**15e pièce**



[https://www.plurielmateriel.com/fr/accessoires-reseaux/118782-989961-rj45-cat-6ase-stp-lot-de-8-4059496559543.html?srsltid=AfmBOor9ZpHLgBI5-5HP3qDAsCxPdDI\\_t88cRWtz7P0y78\\_U2CtKuW2e\\_NA](https://www.plurielmateriel.com/fr/accessoires-reseaux/118782-989961-rj45-cat-6ase-stp-lot-de-8-4059496559543.html?srsltid=AfmBOor9ZpHLgBI5-5HP3qDAsCxPdDI_t88cRWtz7P0y78_U2CtKuW2e_NA)

## ROCADE FIBRE :



Tiroir fibre 12 FO en LC > **120e pièce**

<https://www.zicom.fr/tiroir-optique-equipe-de-12-traversees-lc-duplex-monomode-6.html>

<https://www.fs.com/fr/products/50013.html>

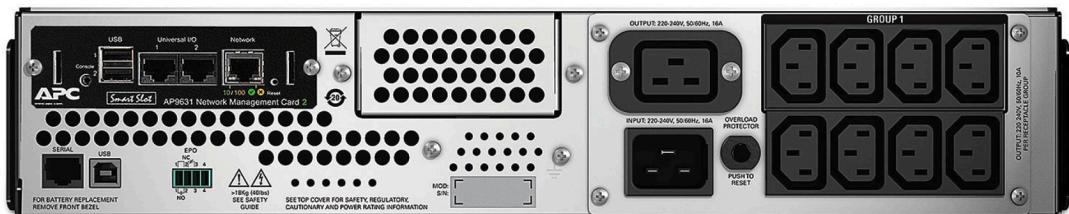
PigTail LC > **2e pièce**

## SWITCH :



Cisco 2960-XR 48 ports POE Manadgeable > **3500e**

## ONDULEUR :



APC Smart-Ups rackable 8 alim intégrés 3000VA 230V > **3400e**

[https://www.ldlc.com/fiche/PB00255033.html?utm\\_source=Ads&utm\\_medium=cpc&utm\\_campaign=Google+Ads&gad\\_source=1](https://www.ldlc.com/fiche/PB00255033.html?utm_source=Ads&utm_medium=cpc&utm_campaign=Google+Ads&gad_source=1)

ROUTEUR 4G :



Cisco C892-LTE > ~**3000e**

<https://www.melbourneglobal.com.au/ge-sfp-vdsl2-adsl2-over-pots-non-us-4/>

ROUTEUR :



Cisco ASR 1001 > **2800e**

<https://www.amazon.fr/Cisco-1001-Ethernet-Routeur-connect%C3%A9/dp/B0064D67D6>

TRANSCEIVER FIBRE/RJ45 (SI BESOIN) :



Transceiver TP\_LINK 1000BASE-T > **32e**  
<https://www.boulanger.com/ref/9000122991>

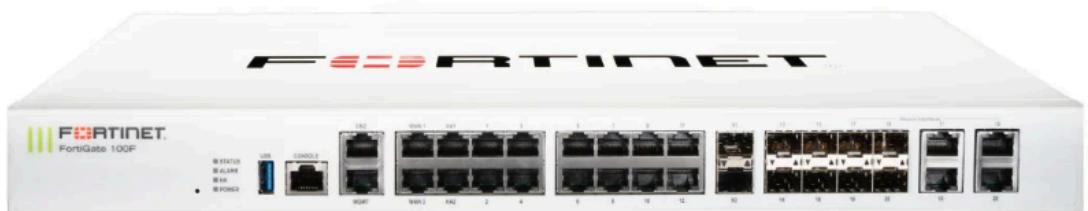
MODULE SFP :

Pour raccordement fibre sur Switch, routeur ou transceiver.



MA-SFT-1GB-LX10 Startech en LC > **100e**  
<https://www.startech.com/fr-fr/entree-sortie-industrielle/masfp1gblx10>

## FIREWALL :



Fortinet FG-100-F > **2140e**

[https://it-planet.com/fr/p/fortinet-fg-100f-389016.html?number=8380937000&gad\\_source=1](https://it-planet.com/fr/p/fortinet-fg-100f-389016.html?number=8380937000&gad_source=1)

## SERVEUR :



DELL PowerEdge XE9680 > **10000e**

<https://www.dell.com/fr-fr/shop/ipovw/poweredge-xe9680>

BAIE :



Baie 42u BueLan  
> **1350e**

<https://www.bureautique-communication.fr/ext-baie-cabling-bluelan-sans-flancs-42u-800-800-1.html>

TOTAL :

Baie coeur de réseau :

- 2 ROUTEURS > **5600 euros**
- Firewall > **2140 euros**
- Serveur > **10000 euros**
- Onduleur > **3400 euros**
- Bandeau Fibre pour rocade > **120 euros**
- Pigtail (environ 12) > **24 euros**
- Modules SFP (environ 8) > **800 euros**
- Baie > **1350 euros**

**TOTAL : 23 434 euros (Sans compter Fibres et cordons de brassage)**

Baie autres sites :

- 1 routeur 4g > **3000 euros**
- 1 routeur > **2800 euros**
- Bandeau fibre pour rocade > **120 euros**
- Pigtail (environ 12) > **24 euros**
- Onduleur > **3400 euros**
- Transceiver FIBRE/RJ45 > **32 euros**
- SWITCH 48P selon nb d'équipements > **Minimum 3500 euros**
- Baie > **1350 euros**
- Modules SFP (environ 4) > **400 euros**

**TOTAL : 14 626 (Avec 1 Switch et sans compter Fibres et cordons de brassage)**

## **5. Proposition d'évolution :**

### **Répartition de charge :**

Nous proposons de mettre en place des mécanismes de répartition de charge avec deux routeurs fibre.

### **Authentification WI-FI avec RADIUS :**

La mise en place d'authentification afin de sécuriser l'accès au WI-FI.

### **AD :**

La mise en place d'un serveur AD permettrait de créer et gérer les droits des utilisateurs, de plus les connexions avec le Wi-Fi pourront être 'loggé'

### **Formation des utilisateurs :**

Avec une formation sur les bonnes pratiques avec internet, le réseau sera d'autant plus sécurisé.

## 6. Glossaire

### DHCP :

La fonction Dynamic Host Configuration Protocol (DHCP) est un protocole client/serveur qui fournit automatiquement une adresse Internet Protocol (IP) et d'autres informations de configuration pertinentes à un hôte IP (par exemple, masque de sous-réseau et passerelle par défaut)

### OSPF :

Le protocole OSPF est un protocole de routage dynamique IGP (Interior Gateway Protocol), à état de liens qui est ouvert.

### ACL :

Une liste de contrôle d'accès, souvent abrégée en ACL, est une liste qui peut être définie comme un ensemble de règles. Ces règles sont conçues pour fournir un certain niveau de contrôle sur l'accès à un réseau ou à un système. Tout d'abord, l'ACL détermine qui peut accéder à quelles ressources et quelles opérations peuvent être effectuées sur ces ressources. Cette liste peut contenir des utilisateurs, des groupes ou des entités informatiques telles que des processus ou des appareils.

### QoS :

La qualité de service (QoS) est l'utilisation de mécanismes ou de technologies fonctionnant sur un réseau pour contrôler le trafic et assurer la performance des applications critiques avec une capacité réseau limitée. Elle permet aux organisations d'ajuster leur trafic réseau global en hiérarchisant des applications haute performance spécifiques.

### Tunnel IPSEC :

IPsec est un groupe de protocoles dont l'objectif est de sécuriser les connexions entre les appareils. IPsec sécurise les données envoyées sur les réseaux publics. Il est souvent utilisé pour mettre en place des VPN, et son fonctionnement prévoit le chiffrement des paquets IP, et l'authentification de la source des paquets.

### SSH

Le protocole Secure Shell (SSH) est une méthode permettant d'envoyer en toute sécurité des commandes à un ordinateur sur un réseau non sécurisé. SSH a recours à la cryptographie pour authentifier et chiffrer les connexions entre les appareils.

## TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) est un protocole permettant de fournir du contrôle d'accès pour les routeurs, les accès réseaux et autres équipements réseaux grâce à un ou plusieurs serveurs centralisés. TACACS+ est un protocole AAA (authentification, autorisation et traçabilité).

## SNMP

Simple Network Management Protocol (SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

## WPA2-PSK

WPA2-PSK est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil, notamment les réseaux domestiques et de petites entreprises. Il est basé sur le protocole WPA2, qui est une amélioration de la norme WPA précédente.

WPA2-PSK fonctionne en utilisant une clé pré-partagée (PSK) pour chiffrer le trafic réseau. La PSK est une phrase secrète qui doit être partagée entre tous les appareils qui se connectent au réseau.

*La définition nous est proposée par BARD, l'intelligence artificielle de Google*

## HSRP :

Hot Standby Router Protocol (HSRP) est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service. HSRP est principalement utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.