PUY DU FOU®

Dossier U5

Mission 2

Ce document présente ma deuxième mission concernant la mise en place d'une segmentation réseau pour un des sites du parc.

GOBERT PIERRE-LOUIS
BTS SIO - OPTION A - SISR
CANDIDAT
N°02046022493
SESSION 2026

UIMM PÔLE FORMATION LA FABRIQUE DE L'AVENIR

Fab Academy PAYS DE LA LOIRE

Tables des matières

PARTIE 1

Présentation du projet

1.1 Contexte

Dans le cadre d'une intervention dans l'entreprise, deux switches Alcatel-Lucent Enterprise OmniSwitch OS6450-P10 ont été déployés pour segmenter et sécuriser le réseau d'un service.

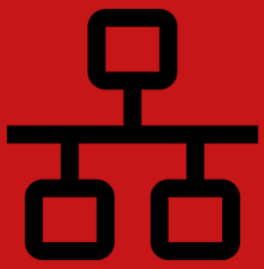
L'objectif était de séparer les flux (postes utilisateurs, administration réseau, téléphonie IP) afin d'améliorer :

- la sécurité (isolement du management, limitation des accès),
- la stabilité (réduction des domaines de broadcast),
- la qualité de service (TOIP isolée),
- et l'exploitabilité (administration centralisée en SSH).

Les équipements ont été installés avec un plan de ports validé et des VLAN normalisés, puis testés en conditions réelles sur site.

GOBERT PIERRE-LOUIS
DATE 30/01/2026

1.2 Expression du besoin



L’administrateur système & réseaux de l’entreprise a exprimé les besoins suivants :

1. Segmentation du réseau en 3 VLAN

- VLAN 10 — Utilisateurs (PC) : postes de travail du service.
- VLAN 20 — Management (MGT) : administration des équipements réseau, réservé au personnel habilité.
- VLAN 30 — Téléphonie IP (TOIP) : trafic voix séparé pour assurer la qualité et la sécurité.

2. Administration sécurisée

- Accès administration uniquement via SSH (telnet interdit).
- Comptes nominatifs / compte technique de gestion (selon politique interne).
- Possibilité d’administrer les switches depuis les ports dédiés 9 et 10 (VLAN 20).

3. Adressage de management

- Switch 1 : 192.168.1.90/24 sur VLAN 20
- Switch 2 : 192.168.1.91/24 sur VLAN 20

4. Plan de ports imposé (contraintes techniques)

- Pour répondre aux contraintes de câblage et d’exploitation (postes, téléphones, brassage), l’affectation des ports devait être :

- Switch 1
- Ports 1 à 4 → VLAN 10 (PC)
- Ports 5 à 6 → VLAN 30 (TOIP)
- Ports 9 & 10 → VLAN 20 (MGT)

Switch 2

- Ports 1 à 4 → VLAN 10 (PC) untagged
- Ports 3 & 4 → VLAN 30 taggé (téléphone IP + PC derrière)
- Ports 9 & 10 → VLAN 20 (MGT)
- Port 10 → interconnexion entre les deux switches

GOBERT PIERRE-LOUIS
DATE 30/01/2026

1.3 Objectifs

- Mettre en service les VLAN demandés et appliquer le plan de ports.
- Garantir que l'administration des switches fonctionne depuis le VLAN 20, en local (ports 9/10) et via l'interconnexion.
- Valider le fonctionnement "téléphone + PC derrière" :
  - PC en VLAN 10 (untagged)
  - Téléphone en VLAN 30 (tagged 802.1Q)
- Vérifier la conformité : commandes de contrôle, tests ping/SSH, preuves via table MAC.

x2

GOBERT PIERRE-LOUIS
DATE 30/01/2026

PARTIE 2

Études et choix de la solution

2.1 Analyse du besoin et contraintes

L'entreprise souhaite une infrastructure réseau simple à exploiter mais conforme aux bonnes pratiques :

- Séparer les usages : utilisateurs / management / téléphonie IP.
- Sécuriser l'administration : limiter l'accès aux équipements à un VLAN dédié, avec SSH uniquement.
- Respecter un plan de brassage : ports imposés (1–6 pour usages, 9–10 pour management), et une interconnexion entre switches.
- Préparer l'intégration TOIP : cas réel "téléphone IP + PC derrière" sur les ports 3/4 du switch 2.

Contraintes techniques :

- Équipements en place : 2 switches OmniSwitch OS6450-P10.
- Adressage management imposé :
  - SW1 = 192.168.1.90/24
  - SW2 = 192.168.1.91/24
- Administration via ports 9 & 10 (VLAN 20).
- Interconnexion via port 10 entre switches.

GOBERT PIERRE-LOUIS
DATE 30/01/2026

2.2 Principe de fonctionnement VLAN / tagged / untagged

Solution	Description	Pourquoi en enterprise ?
Untagged (port access)	Un port untagged transporte des trames sans étiquette VLAN. Le VLAN est déterminé par le port (PVID) : c'est le mode attendu pour un poste de travail ou une imprimante.	• Aucun paramétrage côté PC. • Moins d'erreurs (un PC ne gère pas nativement 802.1Q). • Port dédié à un seul VLAN (usage simple).
Tagged (802.1Q)	Un port tagged ajoute une étiquette VLAN dans la trame Ethernet. Cela permet de transporter plusieurs VLAN sur un même lien.	• Interconnexion entre équipements réseau (trunk). • Cas réel TOIP : téléphone IP tagged la voix (VLAN 30)

GOBERT PIERRE-LOUIS
DATE 30/01/2026

2.3 Choix de la solution retenue

Après analyse, la solution retenue est une segmentation simple en 3 VLAN avec un plan de ports clair et des règles d'administration basiques mais sécurisées.

a) Organisation des VLAN

- VLAN 10 (PC) : dédié aux postes utilisateurs. Les ports sont configurés en untagged pour rester compatibles avec n'importe quel PC (aucune config côté poste).
- VLAN 20 (MGT) : dédié uniquement à l'administration des switches. Les IP 192.168.1.90 et 192.168.1.91 sont portées par l'interface de management sur ce VLAN.
- VLAN 30 (TOIP) : dédié aux téléphones IP. Sur le switch 2, il est utilisé en tagged sur certains ports pour supporter le cas "téléphone + PC derrière".

b) Choix Tag / Untag (pour le cas téléphone + PC)

- Sur un port "téléphone" (SW2 ports 3/4), le choix est :
- PC en VLAN 10 untagged (trafic normal du poste),
- Téléphone en VLAN 30 tagged (le téléphone tagge la voix).
- Ce montage permet un seul point de brassage, tout en séparant data et voix.

c) Administration

Administration via ports dédiés VLAN 20 (9/10) pour éviter de gérer l'admin depuis le VLAN utilisateurs.
Accès distant en SSH, services inutiles réduits (telnet non utilisé).

GOBERT PIERRE-LOUIS
DATE 30/01/2026

PARTIE 3

Planification et organisation

3.1 Étapes du projet

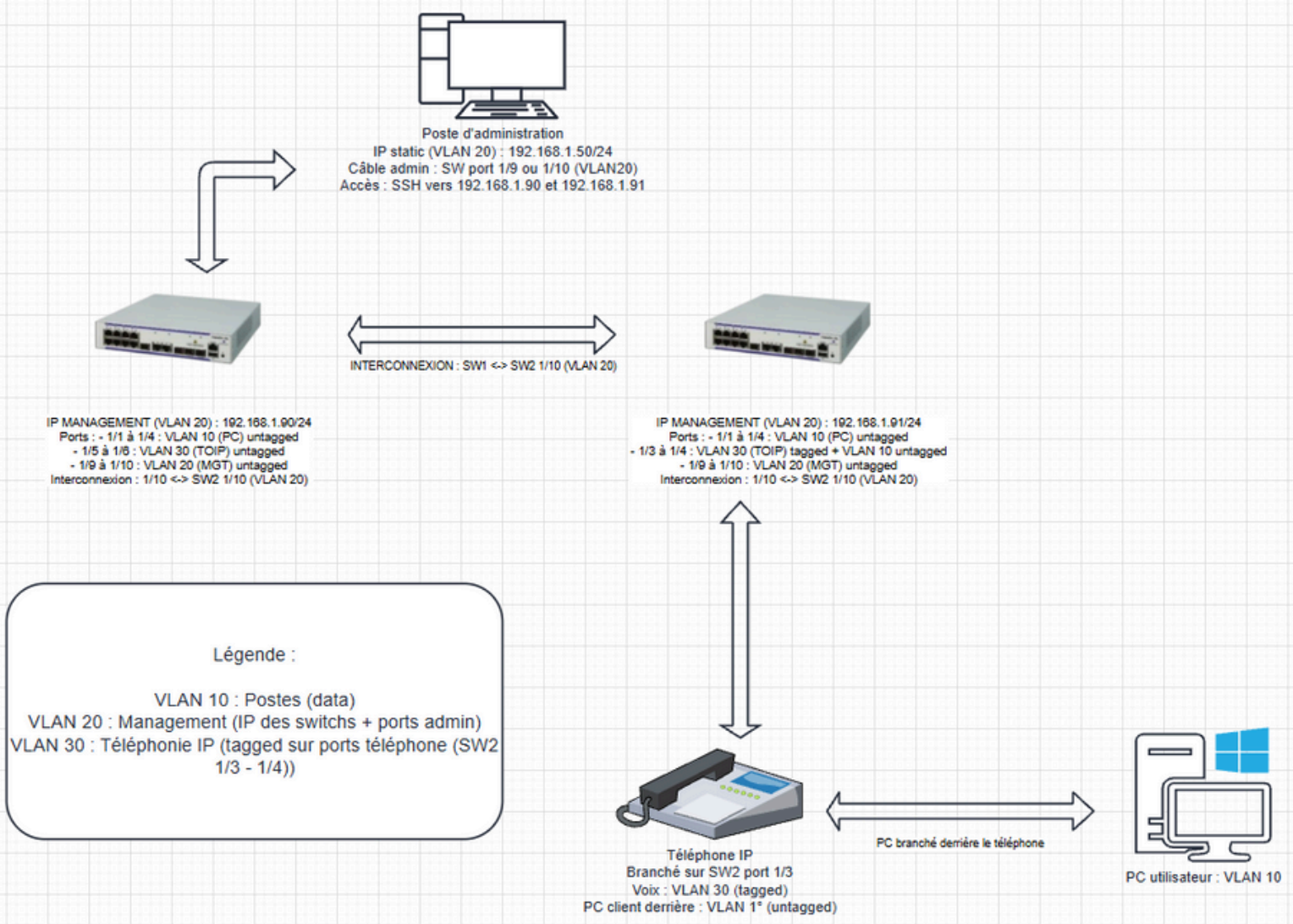
1. Contrôle initial des switches
- Objectif : vérifier versions, VLAN existants, interfaces IP, état config.
2. Mise en place / validation des VLAN
- Objectif : VLAN 10/20/30 présents et activés.
3. Affectation des ports selon cahier des charges
- Objectif : ports PC, TOIP, MGT corrects, et tag TOIP sur SW2 ports 3/4.
4. Configuration/validation du management (VLAN 20)
- Objectif : IP mgmt OK, connectivité inter-switch OK.
5. Activation et validation SSH
- Objectif : accès admin opérationnel depuis un poste branché en VLAN 20.
6. Sauvegarde de configuration
- Objectif : config persistante (working → certified).
7. Tests + preuves
- Objectif : ping inter-switch, ping/SSH depuis poste, preuve tag/untag via table MAC.

3.2 Materiels et logiciels utilisées

Matériel / Logiciel	Description
2 switches OS6450-P10 	Permet de connecter plusieurs appareils (ordinateurs, imprimantes, caméras IP, etc.) au sein d'un même réseau local appelé LAN.
Poste clients (Windows 11) 	Utilisateur du parc
Accès console + câble RJ45 	Accès à la console du switch à l'aide d'un câble rj45 + adaptateur COM & Interconnexion switchs & accès internet pour les postes concernés
Téléphone IP 	Poste téléphonique d'un utilisateur concerné par l'installation

GOBERT PIERRE-LOUIS
DATE 30/01/2026

3.3 Schéma réseau



GOBERT PIERRE-LOUIS
DATE 30/01/2026

PARTIE 4

MISE EN ŒUVRE TECHNIQUE

4.1 État initial des switches

Avant de configurer, on vérifie l'état des deux switches : modèle/OS, VLAN présents, IP configurées, et état de la config (working/certified). Ça sert de référence "avant/après" et évite de partir sur de mauvaises hypothèses.

```
show system
show vlan
show ip interface
show running-directory
show vlan port
```

Ce qu'on vérifie

- show system : version logicielle + identité de l'équipement.
- show vlan : VLAN existants (au début ça peut être VLAN 1 seulement ou déjà 10/20/30).
- show ip interface : interface mgmt présente ou non + IP.
- show running-directory : savoir si la config est bien "certified".
- show vlan port : voir le plan de ports existant.

```
-> show system
System:
  Description:  Alcatel-Lucent Enterprise OS6450-P10 6.7.2.122.R08 GA, September 04, 2020.
  Object ID:    1.3.6.1.4.1.6486.800.1.1.2.1.12.1.2,
  Up Time:      0 days 4 hours 41 minutes and 19 seconds,
  Contact:      Alcatel-Lucent Enterprise, https://www.al-enterprise.com,
  Name:         vxTarget,
  Location:     Unknown,
  Services:     72,
  Date & Time:  THU NOV 30 2000  05:41:28 (UTC)

Flash Space:
    Primary CMM:
      Available (bytes):  47628288,
      Comments          :  None
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

4.2 Création VLAN + affectation des ports

L’objectif est de mettre en place les VLAN demandés puis appliquer la répartition des ports conforme au cahier des charges. (Pour les 2 switchs)

VLAN (contrôle de présence)

```
-> show vlan
                                    stree                          mble   src
 vlan   type   admin    oper    lxl    flat    auth    ip    tag    lrn    name
-----+-----+------+------+------+------+----+-----+-----+------+----------
   1    std    on     off      on     on      off    off    off      on    VLAN 1
  10    std    on      on      on     on      off    off    off      on    PC
  20    std    on      on      on     on      off     on    off      on    MGT
  30    std    on      on      on     on      off    off    off      on    TOIP
```

Affectation des ports Switch 1

```
-> show vlan port
 vlan    port      type       status
------+-------+---------+------------
    1     1/7     default      inactive
    1     1/8     default      inactive
    1     1/11    default      inactive
    1     1/12    default      inactive
   10     1/1     default      inactive
   10     1/2     default      inactive
   10     1/3     default      inactive
   10     1/4     default      inactive
   20     1/9     default      inactive
   20     1/10    default    forwarding
   30     1/5     default      inactive
   30     1/6     default      inactive
```

Affectation des ports Switch 2

```
-> show vlan port
 vlan    port      type       status
------+-------+---------+------------
    1     1/5     default      inactive
    1     1/6     default      inactive
    1     1/7     default      inactive
    1     1/8     default      inactive
    1     1/11    default      inactive
    1     1/12    default      inactive
   10     1/1     default      inactive
   10     1/2     default      inactive
   10     1/3     default    forwarding
   10     1/4     default      inactive
   20     1/9     default      inactive
   20     1/10    default    forwarding
   30     1/3     qtagged    forwarding
   30     1/4     qtagged      inactive
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

4.3 Interface de management (VLAN 20)

Objectif :

S’assurer que chaque switch est administrable via une IP sur le VLAN 20.

```
-> show ip interface
Total 2 interfaces
            Name                   IP Address      Subnet Mask    Status Forward
 Device
-------------------------------+---------------+---------------+------+-------+
-------
Loopback                        127.0.0.1       255.0.0.0           UP      NO
Loopback
mgmt                            192.168.1.90    255.255.255.0       UP      YES
vlan 20
```

4.4 Activation SSH / sécurisation services

Objectif :

Permettre l’administration en SSH avec authentification locale et éviter l’administration en Telnet.
Commandes utilisées (celles qu’on a tapées)

Création compte (exemple : compte admin SSH) :

```
-> user sshadmin password ******** read-write all
```

Activation auth locale SSH + service SSH :

```
-> aaa authentication ssh local
-> ssh enable
-> ip service ssh
->
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

Désactivation telnet (si présent) :

```
-> no ip service telnet
```

Sauvegarde configuration :

```
write memory
copy working certified
show running-directory
```

Commandes de vérification

```
-> show ssh config
SSH = Enabled
SCP/SFTP = Enabled
Public Key Authentication Enforced = False
TCP-Port Number = 22

-> show ip service

  Name                      Port    Status
----------------------+-------+---------
  ftp                       21    enabled
  ssh                       22    enabled
  telnet                    23    disabled
  udp-relay                 67    disabled
  http                      80    disabled
  network-time             123    disabled
  snmp                     161    disabled
  secure-http              443    disabled

-> show aaa authentication
Service type = Default
  Authentication = denied
Service type = Console
  1st authentication server  = local
Service type = Telnet
  Authentication = Use Default,
  Authentication = denied
Service type = Ftp
  1st authentication server  = local
Service type = Http
  Authentication = Use Default,
  Authentication = denied
Service type = Snmp
  Authentication = Use Default,
  Authentication = denied
Service type = Ssh
  1st authentication server  = local
```

```
-> show user
User name = admin,
  Password expiration      = None,
  Password allow to be modified date      = None,
  Account lockout      = None,
  Password bad attempts      = 0,
  Read Only for domains    = None,
  Read/Write for domains   = All ,
  Read Only for view     = None,
  Read/Write for view     = None,
  Snmp allowed      = NO,
  Console-Only     = Disabled,
  Allowed-Configure     = Disabled,
  Password Expiry Notify Period      = None,
User name = default (*),
  Password expiration      = None,
  Password allow to be modified date      = None,
  Account lockout      = None,
  Password bad attempts      = 0,
  Read Only for domains    = None,
  Read/Write for domains   = None,
  Read Only for view     = None,
  Read/Write for view     = None,
  Snmp allowed      = NO,
  Console-Only     = Disabled,
  Allowed-Configure     = Disabled,
  Password Expiry Notify Period      = None,
(*)Note:
  The default user is not an active user account.
  It contains the default user account settings,
  for new user accounts.
User name = sshadmin,
  Password expiration      = None,
  Password allow to be modified date      = None,
  Account lockout      = None,
  Password bad attempts      = 0,
  Read Only for domains    = None,
  Read/Write for domains   = All ,
  Read Only for view     = None,
  Read/Write for view     = None,
  Snmp allowed      = NO,
  Console-Only     = Disabled,
  Allowed-Configure     = Disabled,
  Password Expiry Notify Period      = None,
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

Commandes de vérification

```
-> show ssh config
SSH = Enabled
SCP/SFTP = Enabled
Public Key Authentication Enforced = False
TCP-Port Number = 22
```

```
-> show ip service

  Name                      Port    Status
----------------------+-------+---------
  ftp                       21    enabled
  ssh                       22    enabled
  telnet                    23    disabled
  udp-relay                 67    disabled
  http                      80    disabled
  network-time             123    disabled
  snmp                     161    disabled
  secure-http              443    disabled
```

On remarque bien que :

- SSH enabled
- Port 22 enabled
- Auth SSH sur local
- Compte sshadmin présent
- Config bien CERTIFIED

```
-> show aaa authentication
Service type = Default
  Authentication = denied
Service type = Console
  1st authentication server  = local
Service type = Telnet
  Authentication = Use Default,
  Authentication = denied
Service type = Ftp
  1st authentication server  = local
Service type = Http
  Authentication = Use Default,
  Authentication = denied
Service type = Snmp
  Authentication = Use Default,
  Authentication = denied
Service type = Ssh
  1st authentication server  = local
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

PARTIE 5

TESTS & VALIDATION

5.1 Tests inter-switch (connectivité management)

Objectif :

Vérifier que les deux switches communiquent sur le VLAN 20 (management) via l'interconnexion (port 10 ↔ port 10), et que les IP de management sont joignables.

Test ping réalisé depuis Switch 2 vers Switch 1

```
-> ping 192.168.1.90
PING 192.168.1.90: 56 data bytes
64 bytes from 192.168.1.90: icmp_seq=0. time=167. ms
64 bytes from 192.168.1.90: icmp_seq=1. time=2. ms
64 bytes from 192.168.1.90: icmp_seq=2. time=2. ms
64 bytes from 192.168.1.90: icmp_seq=3. time=22. ms
64 bytes from 192.168.1.90: icmp_seq=4. time=2. ms
64 bytes from 192.168.1.90: icmp_seq=5. time=17. ms
----192.168.1.90 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/35/167
```

Test ping réalisé depuis Switch 1 vers Switch 2

```
-> ping 192.168.1.91
PING 192.168.1.91: 56 data bytes
64 bytes from 192.168.1.91: icmp_seq=0. time=10. ms
64 bytes from 192.168.1.91: icmp_seq=1. time=2. ms
64 bytes from 192.168.1.91: icmp_seq=2. time=2. ms
64 bytes from 192.168.1.91: icmp_seq=3. time=2. ms
64 bytes from 192.168.1.91: icmp_seq=4. time=2. ms
64 bytes from 192.168.1.91: icmp_seq=5. time=2. ms
----192.168.1.91 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/3/10
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

5.2 Tests management (poste Windows)

Objectif

Prouver qu'un poste branché sur un port VLAN 20 peut :

- joindre les 2 switches,
- et se connecter en SSH pour administrer.

Pré-requis (côté poste)
Branchement : PC sur port 9 ou 10 d'un switch (port en VLAN 20).
Configuration IP statique (pas de DHCP) :

- IP : 192.168.1.50
- Masque : 255.255.255.0

```
C:\Users\plgobert>ping 192.168.1.90

Envoi d'une requête 'Ping'  192.168.1.90 avec 32 octets de données :
Réponse de 192.168.1.90 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.1.90 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.90 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.90 : octets=32 temps=8 ms TTL=64

Statistiques Ping pour 192.168.1.90:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 8ms, Moyenne = 3ms
```

Ping vers Switch 1

```
C:\Users\plgobert>ping 192.168.1.91

Envoi d'une requête 'Ping'  192.168.1.91 avec 32 octets de données :
Réponse de 192.168.1.91 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.1.91 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.91 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.91 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.1.91:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
```

Ping vers Switch 2

GOBERT PIERRE-LOUIS
DATE 30/01/2026

SSH vers Switch 1

```
C:\Users\plgobert>ssh sshadmin@192.168.1.90
(sshadmin@192.168.1.90) sshadmin's password for keyboard-interactive method:

Welcome to the Alcatel-Lucent Enterprise OmniSwitch 6450
Software Version 6.7.2.122.R08 GA, September 04, 2020.

Copyright (C) ALE USA Inc. 2014-2019. All rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent Enterprise registered
in the United States Patent and Trademark Office.

->
```

SSH vers Switch 2

```
C:\Users\plgobert>ssh sshadmin@192.168.1.91
(sshadmin@192.168.1.91) sshadmin's password for keyboard-interactive method:

Welcome to the Alcatel-Lucent Enterprise OmniSwitch 6450
Software Version 6.7.2.122.R08 GA, September 04, 2020.

Copyright (C) ALE USA Inc. 2014-2019. All rights reserved.

OmniSwitch(TM) is a trademark of Alcatel-Lucent Enterprise registered
in the United States Patent and Trademark Office.

->
```

GOBERT PIERRE-LOUIS
DATE 30/01/2026

5.3 Preuve Tag/Untag (Switch 2 — téléphone + PC derrière)

Objectif
Démontrer que sur SW2 port 3 (ou 4), on a bien :

- VLAN 10 en untagged pour le PC,
- VLAN 30 en tagged pour le téléphone IP,
- sur un seul câble.

ÉTAPE 1 — PREUVE DE CONFIGURATION (SUR SW2)

```
-> show vlan port
 vlan    port      type       status
------+-------+---------+-------------
    1     1/5     default      inactive
    1     1/6     default      inactive
    1     1/7     default      inactive
    1     1/8     default      inactive
    1     1/11    default      inactive
    1     1/12    default      inactive
   10     1/1     default      inactive
   10     1/2     default      inactive
   10     1/3     default    forwarding
   10     1/4     default      inactive
   20     1/9     default      inactive
   20     1/10    default    forwarding
   30     1/3     qtagged    forwarding
   30     1/4     qtagged      inactive
```

- **VLAN 10 : PORT 1/3 EN DEFAULT (UNTAGGED)**
- **VLAN 30 : PORT 1/3 EN QTAGGED (TAGGED)**

GOBERT PIERRE-LOUIS
DATE 30/01/2026

ÉTAPE 2 — PREUVE DE FONCTIONNEMENT (APPRENTISSAGE MAC)

Branchement :

- Téléphone IP sur SW2 port 3
- PC branché derrière le téléphone (port LAN du téléphone)

```
-> show mac-address-table
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type       Protocol    Operation     Interface
  ------+------------------+--------------+-----------+------------+-----------
    10     fc:5c:ee:8d:8c:22        learned         ---       bridging       1/3
    30     2c:fa:a2:5b:d2:0f        learned         ---       bridging       1/3

Total number of Valid MAC addresses above = 2
```

Sur le même port (1/3) le switch apprend :

une MAC correspondant au PC (dans VLAN 10),
une MAC correspondant au téléphone (dans VLAN 30).

GOBERT PIERRE-LOUIS
DATE 30/01/2026

6 — AXES D’AMÉLIORATION

Objectif : proposer des améliorations réalistes “entreprise”, sans refaire le projet.

6.1 Sécurisation de l’administration

- Désactiver les services inutiles : garder SSH, désactiver telnet/ftp/http si non nécessaires.
- Politique comptes : garder un compte admin principal + supprimer les comptes temporaires.

show ip service (si tu veux prouver que seuls les services utiles sont actifs)

GOBERT PIERRE-LOUIS
DATE 30/01/2026

6.2 Sauvegarde / reprise

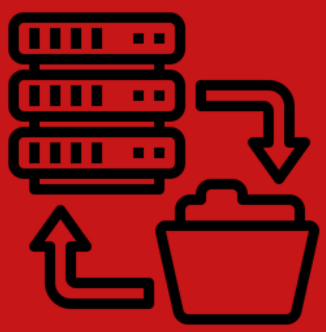
- Exporter la configuration (copie externe) ou, au minimum, vérifier que la configuration est bien en CERTIFIED afin de garantir un redémarrage sans perte.
- Mettre en place une convention de nommage (nom du switch + site/localisation) pour faciliter l'exploitation et le dépannage.

Pourquoi "CERTIFIED" est important ?

Sur OmniSwitch, la configuration active peut être en working (en cours de modification) mais n'est pas forcément celle qui sera reprise au reboot. Le statut CERTIFIED signifie que la configuration a été enregistrée et validée comme configuration de référence : en cas de redémarrage ou coupure, le switch recharge cette configuration "certifiée", ce qui évite de perdre les VLAN, l'IP de management ou la configuration des ports.

6.3 Horloge / logs

- Configurer un NTP pour avoir des logs datés correctement (utile en diagnostic).



GOBERT PIERRE-LOUIS
DATE 30/01/2026

7 — DIFFICULTÉS RENCONTRÉES & SOLUTIONS

7.1 Compatibilité / accès SSH

- Problème : incompatibilité de négociation SSH selon la version logicielle (algorithmes de clés/hostkey).
- Impact : connexion SSH impossible depuis Windows sur un switch.
- Solution : activation/configuration correcte du service SSH + compte local, et mise en conformité de la configuration (vérification via show ssh config et connexion réussie).

7.2 Authentification / comptes

- Problème : politiques de mot de passe / historique empêchant certaines modifications.
- Impact : difficulté à standardiser les accès.
- Solution : création d'un compte admin dédié fonctionnel pour l'exploitation, puis sauvegarde certified.

GOBERT PIERRE-LOUIS
DATE 30/01/2026

PARTIE 8

Conclusion & remerciements

En résumé, cette mission illustre une mise en œuvre concrète et opérationnelle d'une segmentation réseau répondant à un besoin réel en entreprise : séparer les usages (postes, administration, téléphonie) pour améliorer la sécurité, la lisibilité et l'exploitation au quotidien.

La configuration des deux switches Alcatel-Lucent OmniSwitch a permis de mettre en place les VLAN 10/20/30, de rendre l'administration accessible de manière sécurisée via le VLAN management + SSH, et de valider le cas d'usage TOIP "téléphone + PC derrière" grâce au principe tag/untag.
Les tests réalisés confirment la conformité de la solution : connectivité inter-switch, accès management fonctionnel, et preuve du transport simultané des VLAN sur un même port par l'apprentissage MAC (PC en VLAN 10 et téléphone en VLAN 30 sur l'interface concernée).

Au-delà de la configuration, cette mission met en avant l'importance d'une méthode rigoureuse (contrôles, mise en œuvre, validation, sauvegarde) et d'une documentation claire pour assurer la fiabilité et la reprise en conditions professionnelles.

GOBERT PIERRE-LOUIS
DATE 30/01/2026

Je tiens à remercier mon tuteur, l'administrateur système et réseau en entreprise ainsi que mon formateur, pour leur accompagnement, leurs conseils techniques et le temps accordé tout au long de cette mission. Je remercie également l'entreprise pour la confiance accordée et pour la mise à disposition du matériel, qui m'a permis de réaliser cette intervention dans des conditions proches du réel, avec une démarche professionnelle et structurée. Cette expérience constitue un apport concret dans ma progression et dans ma préparation à l'examen.

FLORIAN BARDI & AXEL GAUVRIT & ANTONIN BOLLIN

GOBERT PIERRE-LOUIS
DATE 30/01/2026