BTS SIO
PARCOURS
SISR

Description d'une RÉALISATION PROFESSIONNELLE

compétences E6 ■ Epreuve E6

UFITECH SESSION 2025

Logan **Rochard**
N° CANDIDAT : 02442782589

Recto

N°	INTITULÉ DE LA RÉALISATION PROFESSIONNELLE
1|2	**Cœur De Réseau Switch Infrastructure Réseau Igloonet**

PÉRIODE DE RÉALISATION	MODALITÉ DE RÉALISATION	LIEU DE RÉALISATION
10-2024	[X] **Autonomie** [ ] **Groupe** [ ] **Mode projet**	Labo informatique **07**

COMPÉTENCES TRAVAILLÉES

[X] **Concevoir une solution d'infrastructure**	[X] **Installer, tester, déployer une Solution d'infrastructure**	[X] **Exploiter, dépanner et superviser une solution d'infrastructure**

CONDITIONS DE RÉALISATION (RESSOURCES FOURNIES • RÉSULTATS ATTENDUS)

CONTEXTE GÉNÉRAL : Projet de la **société IGLOONET** fourni par notre professeur et joint en **Annexe 01**.

MÉTHODOLOGIE DE TRAVAIL : Regroupés par 3 étudiants sur un **laboratoire informatique** (schéma topologique joint en **Annexe 02**), notre professeur nous a fixé d'organiser notre travail ainsi :

- **Analyser** le contexte **IGLOONET** et l'expression des besoins en préambule.
- **Travailler**, autant que possible, dans un **mode "orienté projet"** avec, à minima, **l'affectation répartie et synchronisée des tâches** et la **détermination de deadline** (limite) pour chaque tâche.
- S'appuyer sur **une solution de suivi de projet** en ligne (exemple Trello).

OBJECTIFS ET RÉSULTATS ATTENDUS DE LA RÉALISATION :

Les objectifs attendus sont : Savoir configurer les équipements réseaux de niveau 3 et de niveau 2 conformément au plan d'adressage. Savoir configurer les protocoles assurant la haute disponibilité du réseau.
Savoir configurer tout élément d'infrastructure assurant la reprise sur incident

Les résultats et pièces à produire sont : Plan d'adressage IP Igloonet et nomenclature Vlan • Schéma topologique du réseau •Prototypage du protocole HSRP • Jeux de tests réalisés • Dossier des configurations • Documentation "plan de reprise – Incident sur commutateur"
sont :

RESSOURCES DOCUMENTAIRES UTILISÉES	RESSOURCES MATÉRIELLES MOBILISÉES	RESSOURCES LOGICIELLES MOBILISÉES
-Annexe 01 (Présentation du projet IGLOONET) -Documentation des équipements réseau -Documentation sur le protocole HSRP -Cours et supports sur le routage	-Switch de niveau 3 et de niveau 2 -Serveurs labo -NAS (Sauvegarde switch) -Environnement virtualisé proxmox 07	-Simulateur réseau (Packet Tracer, Mob Xtreme) -Systèmes d'exploitation (Windows Server, Linux) -SSH

MODALITÉS D'ACCÈS AUX PRODUCTIONS ET A LEUR DOCUMENTATION

https://loganr06.odoo.com/

Logan **Rochard**
N° CANDIDAT : 02442782589

Verso

DESCRIPTIF DE LA RÉALISATION PROFESSIONNELLE, Y COMPRIS LES PRODUCTIONS RÉALISÉES ET SCHÉMAS EXPLICATIFS

Phase de conception :

Analyser les besoins et les contraintes du projet Igloonet en matière d'infrastructure réseau. (Annexe 03)
- **Rédiger un argumentaire des principales orientations techniques envisagées pour y répondre.** (Annexe 04)
- **Elaborer un plan d'adressage optimisé et associé à une nomenclature des Vlans.** (Annexe 04)
- **Concernant les technologies ou les protocoles les plus sensibles, un prototypage préalable sera attendu** (Annexe 04)
- **Concevoir une infrastructure réseau fiable, sécurisée et évolutive en utilisant des protocoles (Hsrp,Ntp,Vtp,Rstp).** (Annexe 07) (Annexe 08) (Annexe 09) (Annexe 10) (Annexe 11) (Annexe 12)

Phase de configuration et de déploiement :

Configurer les équipements réseaux de niveau 3 et de niveau 2 conformément au plan d'adressage.
Sécurité SSH – Protocole VTP – Les Vlans – Le routage inter Vlan (Annexe 05)
- **Configurer les protocoles assurant la haute disponibilité du réseau.**
  Rapid Spanning Tree (niveau 2) avec une instance par vlan
  – HSRP (niveau 3)
- **Configurer tout élément d'infrastructure assurant la reprise sur incident.** (Annexe 06)
  - Equipement pour la sauvegarde | restauration des configurations des équipements réseau.
  - L'automatisation des sauvegardes TFTP est à prévoir. (Annexe 06)
- **Réaliser les tests de validité.**
- **Rédiger la documentation utilisateur Igloonet décrivant le plan de reprise sur incident de panne d'un commutateur** (Annexe 06)

Phase d'exploitation :
- **L'administration des équipements ne passera que par SSH (à distance) ou par liaison série.** (Annexe 05)
- **Tout incident ou problème significatif devra être documenté après avoir été résolu.**

BILAN DE RÉALISATION • AXES D'ÉVOLUTION| D'AMÉLIORATION

La mise en place de l'infrastructure réseau dans le cadre du projet **Igloonet** a permis de structurer un réseau complet, fiable et sécurisé à l'aide de plusieurs protocoles essentiels au bon fonctionnement d'un cœur de réseau.
Cette réalisation a renforcé la collaboration en mode projet et a permis à chaque membre du groupe d'approfondir ses compétences sur des équipements réseau professionnels Cisco.
Axes d'amélioration et d'évolution : Renforcer la redondance réseau, mettre en place un audit de sécurité sur les équipements actifs

Annexe 1 :

I. Contexte général

La découverte récente d'un virus de type SRAS (Severe Acute Respiratory Syndrome ou Syndrome Respiratoire Aigu Sévère), le SARS-Cov-2, dont la forte propagation en France comme dans de très nombreux pays dans le monde, a créé un contexte pandémique depuis le début de l'année 2020.

Des centaines de milliers de personnes sont contaminées en quelques mois par ce coronavirus (maladie de la Covid-19). Le niveau symptomatique est très varié. Certains cas positifs sont totalement asymptomatiques, d'autres présentent des symptômes bénins mais force est de constater que de nombreux malades développent notamment des complications respiratoires sévères conduisant à leur hospitalisation avec, souvent, un placement en réanimation. Enfin et malheureusement, cette pandémie provoque de très nombreux décès.

a. Contexte sanitaire et dispositions imposées

Cette situation engendre inévitablement de très fortes tensions en milieu hospitalier avec un niveau de saturation rarement atteint. De nombreux états et gouvernements prennent et imposent alors des dispositions drastiques, dont le confinement des populations et la fermeture des commerces, des entreprises, des écoles et des lieux publics, ont été et sont l'un des aspects les plus marquants.

Le monde et ses acteurs font face à un contexte sanitaire, social et économique autant incertain qu'inédit.

b. Conséquences collatérales

Les conséquences d'un tel contexte sont prioritairement d'ordre sanitaire mais impacte fortement l'ordre économique. Les entreprises et les organisations qui le peuvent, envisagent et instaurent massivement le télétravail de leurs collaborateurs. En France notamment, plusieurs observateurs de l'immobilier d'entreprise notent que la répétition des périodes de confinement et la perspective de leur réapparition régulière dans le temps, posent de nouvelles questions stratégiques aux directions générales des entreprises quant à leur politique d'investissement et de gestion de leurs locaux et de leurs bureaux.

Le concept du télétravail, déjà existant mais plutôt marginal, est entré de force dans le mode de fonctionnement des entreprises. Un premier bilan acte qu'il est accepté, qu'il donne des résultats composites mais qui se révèlent néanmoins convenables voir même satisfaisants. Se pose alors mécaniquement la question de l'opportunité de réduire sensiblement les espaces loués et de réexaminer les projets d'extension de nouvelles surfaces locatives.
Il y a donc d'ores et déjà une tension palpable sur le marché de l'immobilier d'entreprises.

c. Opportunités pour Igloonet

C'est ce contexte qui pousse M. Xavier Froid et deux de ses associés, experts et investisseurs immobiliers de profession, à envisager le projet Igloonet.

Ce projet consiste à réaliser justement un investissement immobilier en région parisienne dans des conditions favorables et avantageuses compte tenu des tensions qui se dessinent clairement afin de créer un espace de coworking (espace d'affaires) original qui devra répondre aux nouvelles attentes des entreprises tant au niveau de leur surface d'exploitation que d'une proposition de services intégrés liée aux nouvelles technologies.

Igloonet sera un centre de coworking qui ciblera une clientèle d'entreprises demandeuses de surfaces de bureaux adaptées à des besoins plus restreints et recherchant une infrastructure informatique avancée, évolutive, personnalisée et agile dont elles bénéficieraient comme un service totalement géré.

Pour ce second objectif, Igloonet fonctionnera en quelques sortes comme un datacenter proposant à ses clients de l'IaaS (Infrastructure en tant que Service) avec un mode opérationnel hybride, autrement dit, avec des structures sur site (onpremise) et d'autres à distance (on cloud).

d. Historique

En juin 2020, M. Xavier Froid, Mme Frigide Ere et M. Sam Glace, s'associent et créent à la fois la Société Civile Immobilière (SCI) Igloonet et la Société par Actions simplifiées (SAS) éponyme.

La SCI Igloonet réalise l'acquisition d'un plateau de plein pied d'une surface 2000 m^2 dans le quartier d'affaires de Saint Denis Pleyel.

La SCI Igloonet loue l'intégralité des 2000 m^2 du plateau à la SAS Igloonet qui exploitera l'activité du centre de coworking.

II. L'appel à projet

Pour ce projet, la SAS IglooNet fait un appel concurrentiel à deux ESN (Entreprises de Services du Numérique) afin de répondre au mieux à ses besoins. Les informations fournies à chacune d'elle sont strictement identiques et sont exprimées ci-après :

a. Caractéristiques du plateau

Superficie : 2055 m2
Superficie bureaux : 1 880 m2

- 8 espaces de 40 m2 environ
- 9 espaces de 60 m2 environ
- 6 espaces de 100 m2 environ
- 2 espaces de 200 m2 divisibles en 4 espaces de 45 m2

Espaces communs	: 175 m2 (cuisine, accueil, salle de vie, couloirs…)
Emplacement	: Centre d'affaires de Saint Denis Pleyel (93200)
Niveau(x)	: Plein pied au second étage
Entrée(s)	: 2 entrées principales
Sorties de secours	4
Ascenseurs	2
Toilettes hommes	: 4 au second étage
Toilettes femmes	: 4 au second étage
Installation électrique	: Aux normes et entièrement contrôlée
Câblage réseau	: Oui. Type catégorie 6 FTP (Foiled Twisted Pair)
Prises Ethernet	: 470 (étiquetées et numérotées) - Moyenne : 1 par 4 m2
Brassage	: Oui. 5 baies 19" avec jarretières - Dans local technique de 16 m2

b. Téléphonie
La gestion de la téléphonie IP est exclue du présent appel à projet car elle est prise en charge par un autre prestataire.

c. Espace occupé par la SAS Igloonet
La SAS Igloonet occupera, outre le local technique, un des espaces de 60 m2 mitoyen au local technique.

d. Contraintes liées aux locaux
La SAS Igloonet fixe dans les contrats de location et de services de ses clients une contrainte liée à l'occupation des espaces de travail correspondant à 1 utilisateur par 4 m2 loués avec une tolérance de ± 5%.

e. Type de clients
Les clients de la SAS Igloonet pourront exercer toutes activités licites au regard des lois en vigueur en France et compatibles avec les conditions générales et les conditions détaillées du contrat de location.

Elles seront toutes, avant tout, des entreprises ne possédant pas leur propre système informatique et cherchant à disposer d'une infrastructure informatique réseaux et systèmes en tant que service totalement géré par Igloonet et/ou son prestataire expert habilité.

f. Connexion internet par FAI
La SAS Igloonet a contracté 2 abonnements fibres dédiés à 10Gb symétrique auprès de 2 FAI (Fournisseur d'Accès Internet) distincts, en l'occurrence SFR et ORANGE. En cas de dysfonctionnement, la garantie contractuelle de rétablissement est de 4 heures avec chacun des FAI.
Igloonet possède un pack de 6 adresses IP publiques fixes par FAI.

g. Gestion de projet
Le nom de code du projet est : Igloonet

• Le prestataire ESN retenu sera maitre d'œuvre (MOE) exclusif du projet Igloonet

• Le requérant, maitre d'ouvrage (MOA) seront collectivement M. Xavier Froid, Mme Frigide Ere et M. Sam Glace, associés fondateurs de la SAS Igloonet. Le MOA sera représenté par votre professeur référant.

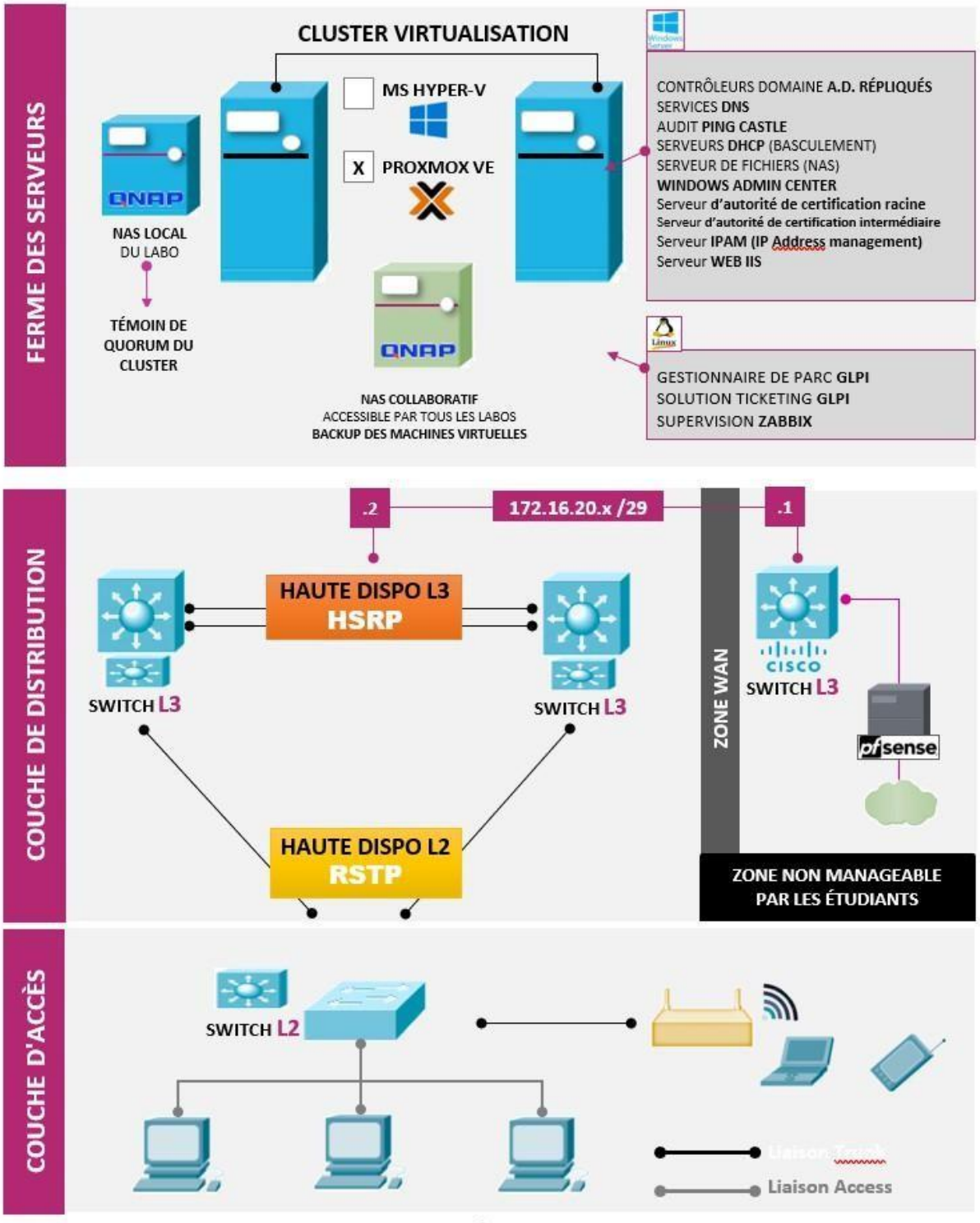
• Des réunions de projet entre le MOA et les membres de l'équipe projet (de manière individuelle ou globale) devront être programmées ainsi que des réunions de projet interne à l'équipe.

III. Expressions des besoins
En liminaire des points détaillés qui suivent, il convient de noter que les axes opérationnels primordiaux que devra intégrer l'infrastructure réseau et système élaborée pour Igloonet à l'attention de ses clients sont :

- La haute disponibilité de l'infrastructure.
- La haute disponibilité des services.
- La sécurisation des données, des accès et des échanges.
- L'archivage des données et des machines virtuelles des clients.
- L'isolation garantie des données et des accès par client.
- Permettre le télétravail en mode sécurisé
- Les performances
- L'agilité à produire à la demande des clients de nouveaux éléments d'infrastructure (commutateurs, machines virtuelles "on premise" ou "on cloud"…) par des outils et des technologies favorisant la méthodologie DevOps.
- L'agilité à faire évoluer à la demande les ressources et les services sollicités et consommés par les clients.
- L'automatisation des tâches d'administration.
- La supervision du système incluant notifications proactives
- Une gestion ITIL des incidents et des demandes d'assistance des clients

Logan **Rochard**
N° CANDIDAT : 02442782589

Annexe 02 — Schéma topologique — LABO 07



Plan d'adressage IPv4 • VLSM

VLAN Id	NOM DU VLAN	RÉSEAU IP / MASQUE	1ÈRE ADRESSE DISPONIBLE	DERNIÈRE ADRESSE DISPONIBLE	PASSERELLE SW L3 ACTIF / PASSERELLE SW L3 STANDBY	PASSERELLE HSRP	BROADCAST
200	Serveur	10.0.13.0 255.255.255.224	1	31	30 29	**28**	31
210	Infrastructure	10.0.13.32 255.255.255.240	33	47	46 45	**44**	47
220	Administration	10.0.13.48 255.255.255.240	49	63	62 61	**60**	63
100	Cisco	10.0.13.64 255.255.255.240	65	75	78 77	**76**	79
110	Alcatel	10.0.13.80 255.255.255.240	81	95	94 93	**92**	95
120	Libre	10.0.13.96 255.255.255.240	97	111	110 109	**108**	111
130	Libre bis	10.0.13.112 255.255.255.240	113	127	126 125	**124**	127
400	Pôle Communication	10.0.13.128 255.255.255.240	129	**143**	**142** **141**	**140**	**143**
410	Pôle RH	10.0.13.144 255.255.255.240	145	**159**	**158** **157**	**156**	**159**
420	Pôle Financier	10.0.13.160 255.255.255.240	161	**175**	**174** **173**	**172**	**175**
430	Pôle Direction/ Gestion	10.0.13.176 255.255.255.240	177	**191**	**190** **189**	**188**	**191**
230	Réplication	10.0.13.192 255.255.255.248	193	**199**	**198** **197**	**196**	**199**
240	Backup	10.0.13.200 255.255.255.248	201	**207**	**206** **205**	**204**	**207**
300	Télécommunication	10.0.13.208 255.255.255.248	209	**215**	**214** **213**	**212**	**215**
310	Imprimantes	10.0.13.2016 255.255.255.248	217	**223**	**222** **221**	**220**	**223**
10	Visiteur	10.0.13.224 255.255.255.248	225	**231**	**230** **229**	**228**	**231**

Annexe 3 :

Analyse des besoins et des contraintes

Besoins identifiés

- **Fiabilité et haute disponibilité**
  L'infrastructure doit garantir un fonctionnement continu, même en cas de panne matérielle.
- **Sécurité renforcée**
  La protection des données et des équipements est primordiale.
- **Gestion centralisée**
  Une administration simplifiée pour la configuration et la supervision du réseau.
- **Évolutivité**
  L'architecture doit pouvoir s'adapter aux besoins futurs sans nécessiter de refonte majeure.
- **Performance optimale**
  Une gestion efficace du trafic et une optimisation des ressources sont nécessaires.

Contraintes techniques

- **Budget limité**
  Il est nécessaire d'optimiser le choix des équipements et des technologies.
- **Compatibilité**
  L'architecture doit pouvoir s'intégrer aux infrastructures existantes tout en restant compatible avec les nouvelles technologies.
- **Maintenance**
  La facilité de mise à jour et de dépannage en cas d'incident est essentielle.
- **Normes et régulations**
  L'ensemble doit respecter les bonnes pratiques ainsi que les réglementations en matière de sécurité et de gestion des données.

Logan **Rochard**
N° CANDIDAT : 02442782589

Annexe 4 :

Argumentaire des principales orientations techniques envisagées

Introduction :

Dans le cadre du projet IGLOONET, il est essentiel de définir une architecture réseau robuste, sécurisée et performante. Ce document présente les orientations techniques retenues pour répondre aux besoins identifiés.

1. Plan d'adressage IP et segmentation en VLAN

Pour garantir une organisation efficace du réseau et assurer une gestion optimale du trafic, nous proposons :

- L'utilisation d'un plan d'adressage IP structurant l'infrastructure en sous-réseaux distincts
- L'implémentation d'une nomenclature VLAN pour segmenter le trafic et renforcer la sécurité.
- La mise en place du protocole VTP (VLAN Trunking Protocol) pour centraliser la gestion des VLANs.
- L'affectation de plages d'adresses IP cohérentes pour faciliter l'administration et le dépannage.

Annexe 5 :

1. Sécurisation des accès avec SSH

L'activation de **SSH (Secure Shell)** permet de sécuriser l'administration à distance des équipements réseau en remplaçant Telnet, qui transmet les informations en clair.

Configuration SSH sur un switch ou un routeur :

1. Activation du protocole SSH avec le domaine **Igloonet.net** :

```
ip domain-name igloonet.net
crypto key generate rsa modulus 2048
ip ssh version 2
```

2. Configuration des accès VTY pour restreindre les connexions à SSH uniquement :

```
line vty 0 4
login local
transport input ssh
transport output ssh
```

```
username admin secret 5 $1$IZ21$pYD5NTwZmC1Smuvo831zT0
```

3. Définition d'un utilisateur avec des droits d'administration :

2. Gestion des VLANs et implémentation de VTP

Le **protocole VTP (VLAN Trunking Protocol)** facilite la gestion des VLANs en permettant leur propagation automatique sur l'ensemble du réseau.

Configuration VTP sur un switch maître (serveur) :

1. Définition du mode VTP avec le domaine **Igloonet.net** :

```
vtp domain igloonet.net
vtp mode server
vtp version 2
vtp password "xxxxxx"
```

2. Ajout et gestion des VLANs :

```
interface Vlan100
 ip address 10.0.13.77 255.255.255.240
```

Annexe 6 :

Sauvegarde automatique avec Kron sur Switch

Cisco via TFTP Objectif

Cette procédure détaille la configuration de l'automatisation des sauvegardes de configuration d'un switch Cisco en utilisant **Kron** pour effectuer la sauvegarde sur un serveur TFTP (NAS). Kron permet de programmer l'exécution de commandes à des intervalles réguliers, offrant ainsi une solution de sauvegarde automatisée.

Prérequis

- Un switch Cisco avec une version qui prend en charge Kron (disponible sur les équipements Cisco exécutant IOS avec une version compatible).
- Un serveur NAS avec un service TFTP actif et un répertoire dédié pour les sauvegardes.

Configuration du Switch Cisco avec Kron

1. **Accéder au mode de configuration du switch Cisco** : Connectez-vous au switch via la console ou SSH, puis entrez en mode privilégié et configurez le switch en mode configuration.

```
enable
configure terminal
```

2. **Vérifier la connectivité réseau du switch vers le serveur TFTP** : Avant de configurer Kron, il est crucial que le switch puisse atteindre le serveur TFTP (NAS). Utilisez la commande ping pour tester la connectivité.

```
ping 10.0.13.3
```

Créer une tâche Kron pour sauvegarder la configuration :

- Kron est utilisé pour programmer des tâches récurrentes. Nous allons créer une tâche qui copie la configuration en cours du switch vers le serveur TFTP à des intervalles réguliers.

```
kron occurrence backup-config at 03:00 recurring
```

Annexe 07 :

Procédure de mise en place du protocole VTP (VLAN Trunking Protocol)

1. Introduction au VTP

Le VTP (VLAN Trunking Protocol) est un protocole Cisco permettant de gérer la propagation automatique des VLANs entre plusieurs commutateurs (switches) d'un même domaine réseau.
Il évite la création manuelle des VLANs sur chaque équipement, en simplifiant l'administration.

Modes principaux du VTP :

- **Server : Crée, modifie et supprime des VLANs. Réplication vers d'autres switches.**
- **Client : Reçoit et applique les VLANs mais ne peut pas modifier.**

2. Configuration étape par étape

Sur le Switch principal (mode Server) :

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vtp domain IGLOONET
Switch1(config)# vtp mode server
Switch1(config)# vtp password igloopass
Switch1(config)# vlan 10
Switch1(config-vlan)# name SERVICE
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name ADMIN
Switch1(config-vlan)# exit
```

Sur les autres Switchs (mode Client) :

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vtp domain IGLOONET
Switch2(config)# vtp mode client
Switch2(config)# vtp password igloopass
```

Important :

- **Le nom de domaine et le mot de passe VTP doivent être les mêmes sur tous les switches.**
- **Les ports reliant les switches doivent être en mode trunk.**

Exemple de configuration du trunk :

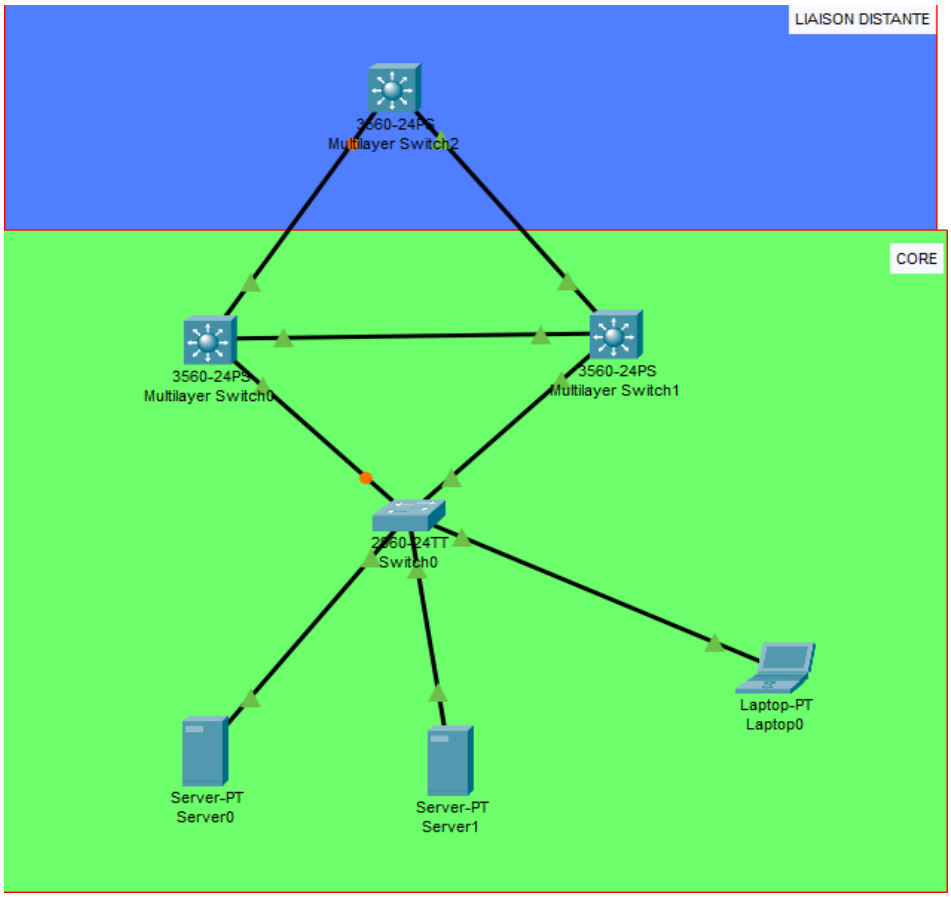
```
Switch1(config)# interface gigabitEthernet0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
```

4. Vérification de la configuration :

Vérifier l'état VTP :

```
Switch1# show vtp status
```

5. Illustration (packet tracer) :



Logan **Rochard**
N° CANDIDAT : 02442782589

Serveur :

```
SWL3/1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : IGLOONET.net
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0004.9AD5.6E00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.0.13.78 on interface Vl100 (lowest numbered VLAN interface
found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 106
MD5 digest                      : 0xE0 0x18 0x1C 0x77 0x82 0x80 0x26 0xC1
                                  0x78 0xD1 0x14 0x57 0xC8 0xB5 0xBB 0xF0
```

Client :

```
SWL2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : IGLOONET.net
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BC17.1900
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
Configuration Revision          : 106
MD5 digest                      : 0xE0 0x18 0x1C 0x77 0x82 0x80 0x26 0xC1
                                  0x78 0xD1 0x14 0x57 0xC8 0xB5 0xBB 0xF0
```

Annexe 08 :

Procédure de mise en place du protocole RSTP (Rapid Spanning Tree Protocol)

1. **Introduction au RSTP :**

Le RSTP (Rapid Spanning Tree Protocol) est une évolution rapide du protocole STP.
Il permet de prévenir les boucles réseau tout en assurant une convergence plus rapide (quelques secondes au lieu de plusieurs dizaines avec STP classique).
Fonctions principales :

- **Évite les boucles en désactivant certains ports si nécessaire.**
- **Réagit très vite en cas de défaillance d'un lien.**

2. **Configuration étape par étape :**

Sur tous les Switchs (activation du mode RSTP) :

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# spanning-tree mode rapid-pvst
```

Définir le Switch racine (Root Bridge) :

```
Switch1(config)# spanning-tree vlan 1 priority 4096
```

Plus la priorité est basse, plus le switch a de chances d'être élu Root Bridge.
(4096 est une priorité faible ; par défaut elle est à 32768.)

3. **Vérification de la configuration**
   Vérifier que RSTP est actif :

```
Switch1# show spanning-tree
```

Vérifier l'état des ports :

```
Switch1# show spanning-tree interface status
```

4. Illustration :

Vérification du Rstp :

```
SWL3/1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     0001.43D6.5C27
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0090.2B28.7403
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/20           Desg FWD 19        128.20   P2p
Gi0/1            Root FWD 4         128.25   P2p

VLAN0100
  Spanning tree enabled protocol rstp
  Root ID     Priority    24676
              Address     0001.43D6.5C27
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24676  (priority 24576 sys-id-ext 100)
              Address     0090.2B28.7403
```

Vérification :

```
SWL3/1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          2          3
VLAN0100                    1         0        0          2          3
VLAN0200                    1         0        0          2          3
VLAN0210                    1         0        0          2          3

---------------------- -------- --------- -------- ---------- ----------
4 vlans                     4         0        0          8         12
```

Annexe 09 :

Procédure de mise en place du protocole HSRP (Hot Standby Router Protocol)

1. **Introduction à HSRP**

Le HSRP (Hot Standby Router Protocol) est un protocole Cisco permettant d'assurer une haute disponibilité au niveau de la passerelle par défaut.
Il permet à deux ou plusieurs routeurs/switches de simuler une passerelle virtuelle commune :

→ Si le routeur principal tombe, un autre prend immédiatement le relais sans couper la connexion.
Fonctions principales :

Fournit une adresse IP virtuelle partagée par plusieurs équipements.
Un routeur actif (Active Router) gère normalement la passerelle.
Un routeur en attente (Standby Router) est prêt à prendre la relève.

2. **Configuration étape par étape**

Sur le routeur (Actif) :

```
Router1> enable
Router1# configure terminal
Router1(config)# interface gigabitEthernet0/0
Router1(config-if)# ip address 192.168.1.2 255.255.255.0
Router1(config-if)# standby 1 ip 192.168.1.1
Router1(config-if)# standby 1 priority 110
Router1(config-if)# standby 1 preempt
```

Sur le routeur (Standby) :

```
Router2> enable
Router2# configure terminal
Router2(config)# interface gigabitEthernet0/0
Router2(config-if)# ip address 192.168.1.3 255.255.255.0
Router2(config-if)# standby 1 ip 192.168.1.1
Router2(config-if)# standby 1 priority 100
Router2(config-if)# standby 1 preempt
```

3. Explication des commandes

- **standby 1 ip 192.168.1.1** : définit l'adresse IP **virtuelle** commune.
- **priority** : plus la priorité est haute, plus le routeur a de chances d'être **actif**.
- **preempt** : permet au routeur de **reprendre la main** s'il retrouve une meilleure priorité (par exemple après un redémarrage).

4.Vérification de la configuration

Sur chaque routeur, pour vérifier l'état HSRP :

```
Router1# show standby
Router2# show standby
```

5. Illustration :

Switch (actif) :

```
SWL3/1#show standby
Vlan100 - Group 200 (version 2)
  State is Active
    7 state changes, last state change 00:00:18
  Virtual IP address is 10.0.13.76
  Active virtual MAC address is 0000.0C9F.F0C8
    Local virtual MAC address is 0000.0C9F.F0C8 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.692 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.13.77
  Priority 150 (configured 150)
  Group name is hsrp-Vl1-200 (default)
Vlan200 - Group 200 (version 2)
  State is Active
    7 state changes, last state change 00:00:27
  Virtual IP address is 10.0.13.28
  Active virtual MAC address is 0000.0C9F.F0C8
    Local virtual MAC address is 0000.0C9F.F0C8 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.621 secs
  Preemption disabled
```

Switch(passif) :

```
Vlan100 - Group 200 (version 2)
  State is Standby
    8 state changes, last state change 00:00:27
  Virtual IP address is 10.0.13.76
  Active virtual MAC address is 0000.0C9F.F0C8
    Local virtual MAC address is 0000.0C9F.F0C8 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.089 secs
  Preemption enabled
  Active router is 10.0.13.78
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Vl1-200 (default)
Vlan200 - Group 200 (version 2)
  State is Standby
    9 state changes, last state change 00:00:39
  Virtual IP address is 10.0.13.28
  Active virtual MAC address is 0000.0C9F.F0C8
    Local virtual MAC address is 0000.0C9F.F0C8 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.48 secs
  Preemption enabled
```

Annexe 10 :

Procédure de mise en place du protocole SNMP (Simple Network Management Protocol)

1. Introduction à SNMP

Le SNMP (Simple Network Management Protocol) est un protocole qui permet de superviser et gérer à distance des équipements réseau (switches, routeurs, serveurs, imprimantes...).
Il est principalement utilisé pour :

- **Surveiller l'état des équipements (trafic, température, utilisation CPU, etc.).**
- **Envoyer des alertes en cas de problème.**
- **Automatiser la gestion réseau.**

Versions principales :

- **SNMPv1 : Basique, pas sécurisé.**
- **SNMPv2c : Plus de fonctionnalités, mais encore sans sécurité.**
- **SNMPv3 : Sécurisé (authentification et chiffrement).**

Configuration étape par étape :

```
Switch> enable
Switch# configure terminal
Switch(config)# snmp-server community igloonet RO
Switch(config)# snmp-server location Salle Serveur
Switch(config)# snmp-server contact admin@igloonet.local
```

Vérification de la configuration :

Vérifier l'état SNMP sur le switch :

```
Switch# show running-config | include snmp
```

Logan **Rochard**
N° CANDIDAT : 02442782589

Annexe 11 :

Procédure de mise en place du protocole NTP (Network Time Protocol)

1. Introduction à NTP

Le NTP (Network Time Protocol) est un protocole utilisé pour synchroniser automatiquement l'heure entre les équipements d'un réseau (switchs, routeurs, serveurs, PC).

La synchronisation d'heure est essentielle pour :

- **Le bon fonctionnement des logs.**
- **La sécurité (authentifications, HSRP, etc.).**
- **Le bon ordre des événements dans le réseau.**

Fonctionnement de base :

- **Un ou plusieurs serveurs NTP fournissent l'heure exacte.**
- **Les équipements clients se synchronisent régulièrement avec ces serveurs.**

Configuration étape par étape :

```
Switch> enable
Switch# configure terminal
Switch(config)# ntp server 192.168.1.100
Switch(config)# clock timezone CET 1
Switch(config)# clock summer-time CEST recurring
```

Vérification de la configuration :

Vérifier l'état de synchronisation :

```
Switch# show ntp status
```

Annexe 12 :

Procédure de mise en place du protocole TFTP (Trivial File Transfer Protocol)

1. Introduction à TFTP

Le TFTP (Trivial File Transfer Protocol) est un protocole de transfert de fichiers léger et simple utilisé principalement pour :

- **Sauvegarder ou restaurer la configuration d'équipements réseau (routeurs, switches, etc.).**

Particularités de TFTP :

- **Fonctionne en UDP (port 69).**
- **Très rapide, mais pas sécurisé (réservé aux réseaux internes fiables).**

2. Exemple de configuration et d'utilisation sur Cisco :
Sauvegarder la configuration d'un switch vers un serveur TFTP

```
Switch> enable
Switch# copy running-config tftp:
Address or name of remote host []? 192.168.1.100
Destination filename [running-config]? sauvegarde-switch.cfg
```

Restaurer une configuration depuis un serveur TFTP vers le switch :

```
Switch> enable
Switch# copy tftp: running-config
Address or name of remote host []? 192.168.1.100
Source filename []? sauvegarde-switch.cfg
Destination filename [running-config]? [ENTER]
```

Sauvegarder ou restaurer un fichier IOS (système d'exploitation Cisco)

Pour sauvegarder l'IOS :

```
Switch# copy flash: tftp:
```

Pour restaurer un IOS :

```
Switch# copy tftp: flash:
```

Vérification de la communication :

Avant de lancer des copies TFTP :

Tester la connectivité réseau :

```
Switch# ping 192.168.1.100
```