

Projet Longue Durée MARS

Table des matières

1	<i>Introduction</i>	3
1.1	Contexte du projet	3
1.2	Domaine d'application	3
2	<i>Tâche 1: Conception de l'architecture de services et de l'architecture technique</i>	3
2.1	Conception d'ensemble	3
2.2	Conception fonctionnelle détaillée	3
2.3	Conception applicative détaillée	4
2.4	Architecture technique et répartition du système d'information	4
2.5	Gestion de projet	4
2.6	Livrables de la tâche 1	5
3	<i>Tâche 2 : Conception de l'architecture distribuée validée par un POC</i>	5
3.1	Architecture retenue pour le POC	5
3.2	Etude d'architecture	6
3.3	Spécifications détaillées et réalisation du POC	7
3.4	Gestion du nommage	7
3.5	Organisation du sous-projet et résultats attendus	8
4	<i>Tâche 3 : présentation de votre offre</i>	8
	<i>Annexes</i>	9
5	<i>Diagramme d'organisation - MCD – CU</i>	10
5.1	Diagramme d'organisation	10
5.2	Modèle conceptuel de données – E-A	11
5.3	Expression des besoins – Situations fonctionnelles	12
5.3.1	CU1 – Consultation du dossier Client : Vue 360°	12
5.3.2	CU2 – Gestion du client (Zone Client)	12
5.3.3	CU3 – Gestion des contacts clients (Zone Relation Banque/Client)	13
5.3.4	CU4 – Gestion des contrats du client (Zone Contrats)	13
6	<i>Détails pratiques pour la mise en œuvre du poc</i>	14
6.1	Câblage de votre banc	14
6.2	Petits détails pratiques	14
6.3	Affectation des adresses IP par hexanome	17
6.4	Affectation des réseaux aux ports des switch d'interconnexion, adresses des routeurs et masque de réseau	18
6.5	Catalogue de machine virtuelle	18
6.6	Livrables attendus	19
7	<i>CAHIER de TP : Mémento sur les étapes à suivre</i>	20
7.1	Conception de l'architecture	21
7.1.1	Organisation du plan d'adressage	21

7.1.2	Organisation de l'architecture globale	22
7.1.3	Organisation du POC sur table	24
7.1.4	Maîtrise de la chaîne de liaison	26
7.1.5	Organisation de l'espace de nommage (facultatif)	27
7.2	Préparation de votre banc	28
7.2.1	Configuration de vos machines	28
7.2.2	Configuration de votre switch	29
7.2.3	Configuration de vos routeurs	29
7.2.4	Configuration des connexions sur un même site	30
7.3	Mise en place d'accès externes pour le télétravail: VPN SSL	33
7.4	Gestion des configurations	34
7.4.1	Organisation du DHCP	34
7.4.2	Organisation du DNS (facultatif)	36

1 INTRODUCTION

8 séances projet : 3 séances de conception de l'architecture de services et de l'architecture techniques, 1 séance de présentation orale de la conception et de préparation du déploiement, 3 séances de conception et implémentation de l'infrastructure réseau, une séance de validation de l'infrastructure.

1.1 *CONTEXTE DU PROJET*

Le projet vise à mettre en application la démarche et les méthodes de conception d'architectures de services distribués et de conception/implémentation d'une infrastructure réseau.

1.2 *DOMAINE D'APPLICATION*

Le cas étudié porte sur « la vue 360° des clients d'une banque ». Les applications à concevoir et l'architecture du poste de travail doivent apporter une aide aux agents commerciaux d'une banque pour :

- gérer les informations du client
- gérer les comptes du client
- permettre d'effectuer un suivi des interactions avec le client et d'identifier de nouvelles interactions à déclencher
- gérer les contrats du client notamment avec les prestataires partenaires issus de différents domaines.

2 TACHE 1: CONCEPTION DE L'ARCHITECTURE DE SERVICES ET DE L'ARCHITECTURE TECHNIQUE

2.1 *CONCEPTION D'ENSEMBLE*

Les résultats attendus sont traduits dans :

- Le modèle conceptuel de données du domaine étudié ; dans le cadre du TP, le MCD étant fourni, on demande uniquement d'analyser les modèles proposés, de les comprendre au regard des CU représentatifs.
- L'identification et la **définition générale des blocs applicatifs** (blocs du noyau applicatif) à concevoir basés sur les OM : **modèles de données découpés en blocs**.

2.2 *CONCEPTION FONCTIONNELLE DETAILLEE*

Les résultats attendus sont traduits dans :

- Le découpage des CU représentatifs en scénarios élémentaires (si nécessaire) et la spécification de ces scénarios sous forme de : **DA (au moins 1 DA/CU)**
- L'identification des principaux services métier applicatifs (SMA) caractérisant l'information échangée entre les utilisateurs et l'architecture logique dans le cadre des CU représentatifs : **DSS (un DSS par DA)**

- La spécification de l'IHM centrée Objets Métier (OM):
 - la description des fenêtres (centrées OM)
 - la liste des SMA invoqués par fenêtre.

2.3 CONCEPTION APPLICATIVE DETAILLEE

Dans le cadre du projet, on limitera les résultats attendus à :

- L'identification des SOM : identification des principaux services invoqués sur les blocs de l'architecture logique sous forme de **DSD (au moins 1 par DSS)**

2.4 ARCHITECTURE TECHNIQUE ET REPARTITION DU SYSTEME D'INFORMATION

Choix de l'environnement technique : l'environnement technique déjà retenu par la Maîtrise d'Ouvrage (MOA) de la banque est une architecture C/S n-tiers web.

La répartition du système d'information précise l'implantation des composants du noyau applicatif sur l'architecture technique. Tout composant du système commercial peut être réparti sur des serveurs du siège ou des agences si nécessaire.

Les **résultats attendus** concernent la spécification de l'architecture technique volet production :

- Identification des serveurs [SA,SD,SP] et nombre, localisation (relativement au diagramme organisationnel) ;
- Implantation des composants du noyau applicatif (blocs et Services Métiers Applicatifs), sur cette architecture technique (préciser si les blocs sont répartis, répliqués...) ;
- Identification des principaux flux (MAJ, Consultation, Sauvegarde, Réplication si nécessaire) applicatifs échangés après répartition des blocs sur l'architecture technique.

2.5 GESTION DE PROJET

Il est demandé aux équipes de s'organiser en mode projet, sous le pilotage d'un chef de projet et d'un responsable qualité.

Chef de projet :

- **effectuer le suivi du projet et l'animation de l'équipe**
 - remplissage de fiches de suivi par tâche (charge réalisée) et par membre de l'équipe
 - harmonisation des livrables et des syntaxes de rédaction (ex : diagramme de séquence)
- **établir un petit document de bilan (total charge réalisée, difficultés rencontrées, critiques positives et négatives) avec le compte-rendu du projet.**

Responsable qualité :

- **assurer la cohérence et l'homogénéité des diagrammes,**
- **intégrer les différents livrables dans le compte-rendu final.**

2.6 LIVRABLES DE LA TACHE 1

Livrables :

- Compte-rendu du projet intégrant les résultats attendus (Conception d'ensemble, conception détaillée, architecture) sous forme d'un unique fichier PDF – NB : les DSS ne sont pas à intégrer (DSD = DSS étendus)
- Bilan chef de projet (à intégrer dans le fichier PDF)
- Présentation orale du projet
- Support de la présentation orale (PDF)

3 TACHE 2 : CONCEPTION DE L'ARCHITECTURE DISTRIBUEE VALIDEE PAR UN POC

Dans une logique d'avant-vente, votre manager vous demande de préparer un « POC » correspondant à la mise en œuvre d'une partie du système d'information d'une entreprise multi-agences, système que vous venez de concevoir.

L'architecture doit favoriser les regroupements de moyens.

La direction souhaite

- pouvoir mutualiser l'exploitation,
- que le site central ou un autre site puisse héberger (temporairement ou non) les ressources allouées usuellement à d'autres entités (maintient en conditions opérationnelles)

L'architecture doit permettre aux entités de bénéficier de services communs pour développer leurs capacités de travail à distance.

Les éléments clefs à interconnecter sont :

- Des postes clients
- Un ensemble de serveurs du système d'information
- Des machines permettant de gérer la configuration et l'exploitation de cette architecture.

3.1 ARCHITECTURE RETENUE POUR LE POC

La solution proposée par l'équipe assurant l'avant-vente est la suivante (figure 1) :

- L'architecture comporte trois familles de sites :
 - un site central est associé à un siège régional. Il héberge le serveur de nommage et la plupart des serveurs de production mais aussi des postes clients.
 - Les agences principales hébergent des postes clients et des automates bancaires. Ces agences peuvent héberger des serveurs relatifs à la gestion de leur clientèle selon les choix faits dans la tâche précédente

- Les agences secondaires n'hébergent que des postes clients et des automates bancaires... Ceux-ci accèdent aux serveurs via une connexion de type VPN.
- Les agences principales sont raccordées au site central grâce à un VPN.
- On désire automatiser le plus possible la gestion des machines et de leur configuration de manière à faciliter l'exploitation (donc de travailler dans une logique dynamique). Chaque site doit être autonome (et donc pouvoir fonctionner en mode dégradé même en cas de coupure de la liaison avec l'autre site)
- les environnements peuvent être différents pour chaque site : (LINUX ou Microsoft Windows).
- Les trafics entre les sous-réseaux différents doivent être séparés de manière à ne pas être pénalisé en termes de performance et augmenter la sécurité
- Vous disposez de 6 adresses IP publics pour vous permettre d'accéder au réseau d'interconnexion (voir section 2.4)
- Un plus pour le client serait de proposer une solution permettant le télétravail. Dans ce cas, il faut que le poste en télétravail puisse utiliser les ressources du siège.

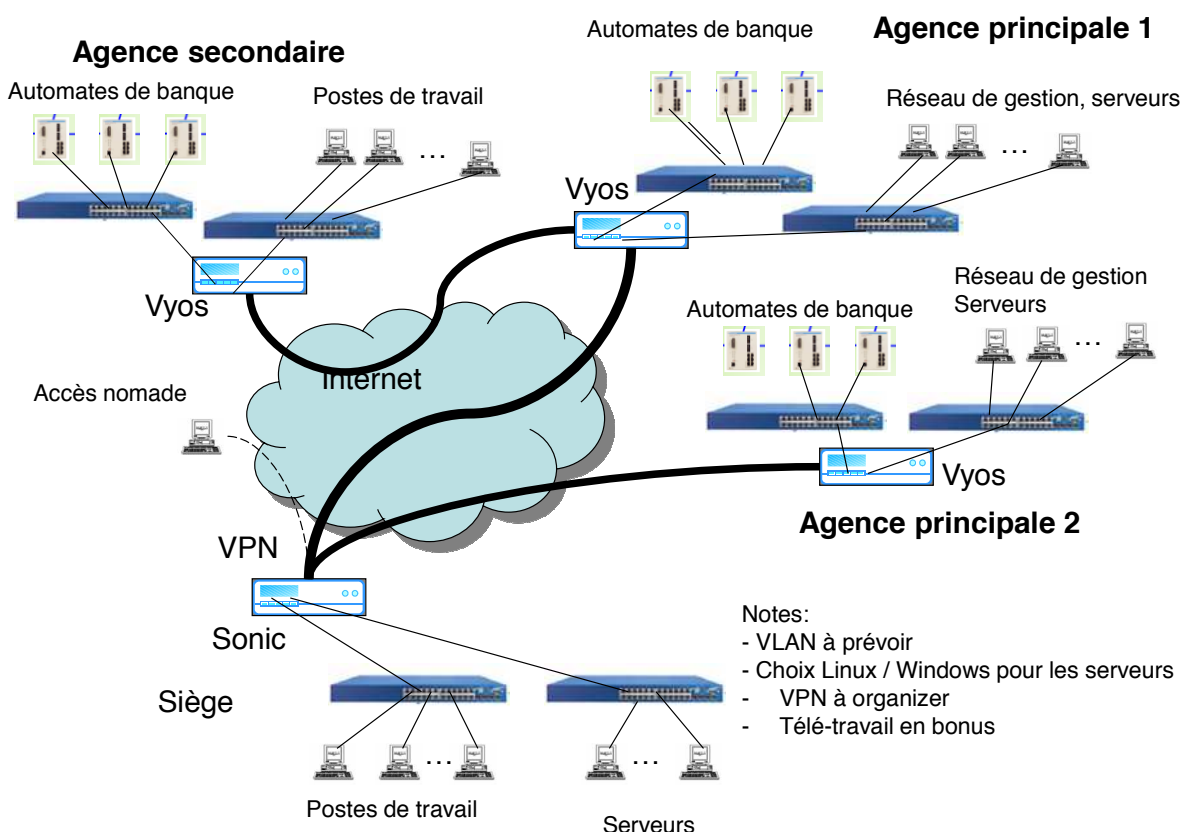


Figure 1 : schéma de principe de l'architecture du POC

3.2 ETUDE D'ARCHITECTURE

De manière à assurer le Proof Of Concept de votre architecture, on vous demande de prototyper les éléments caractéristiques de votre proposition puis de les intégrer. Pour cela, vous devez au préalable préciser les éléments de l'architecture :

- Identification des différentes machines
- Définition des adresses
- Définition des liens d'interconnexion
- Identification des différents flux
- Définition des éléments logiciels à configurer
- Organisation du plan de nommage (zones) : ce point est facultatif

3.3 SPECIFICATIONS DETAILLEES ET REALISATION DU POC

Pour réaliser le POC vous devrez :

- Configurer les équipements d'interconnexion (switch et routeurs) pour permettre la communication sur chaque site puis de manière sécurisée entre les sites. Un réseau d'interconnexion simulant le réseau Internet sera partagé par les différents hexanomes.
- Configurer les différentes machines virtuelles

Pour cela, vous disposez d'une plateforme de TP (repérée comme un Banc) intégrant :

- une machine sous Windows reliée au réseau de production du département Informatique vous permettant d'accéder à Internet en cas de besoin
- machines physique sous Linux Fedora (étiquette Banc X CENTOS Y) dotées de Virtual Box sur lesquelles les machines virtuelles seront exécutées,
- Un switch 3COM propre pour chaque hexanome
- 1 routeur matériel dont vous devrez gérer les sauvegardes des éléments de configuration
- Un ensemble de VM mises à votre disposition sur les machines Fedora.
- Un réseau d'interconnexion fourni et géré par nos soins vous permettant d'accéder au réseau de production du département informatique

Les sauvegardes de vos environnements sont de votre responsabilité. Si vous disposez droits administrateur (log admin pwd TP4if2012) sur ces VM, il n'en est pas de même pour les quatre machines physiques où disposez d'un compte par hexanome sur chaque machine physique. Toutefois un ensemble de commandes SUDO sont mises à votre disposition pour réaliser les nécessaires configurations sur ces machines. Cette solution vous permet de pouvoir travailler sur vos VMs et d'en lancer l'exécution sur les différentes plateformes de la salle une fois configurés vos équipements d'interconnexion.

3.4 GESTION DU NOMMAGE

L'objectif de ce lot facultatif est de définir précisément les éléments technologiques et les processus à mettre en place pour permettre une bonne gestion des fonctions de nommage. Il faut aussi permettre une configuration dynamique des paramètres réseau des différentes machines de manière à assurer la portabilité de votre solution.

Pour répondre au cahier des charges vous devez proposer :

- La mise en place d'une politique de nommage

- La gestion des adresses

La mise en place d'une politique de nommage passe par la création de services d'annuaires adaptés. Dans notre cas, plusieurs sites sont impliqués et doivent disposer de leur propre DNS. Dans votre présentation, vous présenterez l'architecture retenue et les procédures nécessaires pour l'exploitation. Nous vous fournissons un service de nommage au sein de la zone TP4IF. Pour créer vos domaines et que nous vous donnions délégation, vous devez nous transmettre par email (fcetre@openinfra.eu et frederique.biennier@insa-lyon.fr) vos demandes complètes.

3.5 ORGANISATION DU SOUS-PROJET ET RESULTATS ATTENDUS

Le projet est organisé en 3 étapes principales :

- Spécification détaillée de l'architecture :
 - D'identifier les composants réseau à intégrer pour proposer une architecture sécurisée et facilement configurable sur chaque site
 - De proposer une solution d'interconnexion des différents sites permettant de rester compatible avec les contraintes de sécurité propres à chaque site
 - De définir un plan de nommage et d'adressage permettant de faciliter à terme l'exploitation
- Configuration des éléments de la solution
 - Mise en œuvre des différents systèmes
 - Paramétrage des différents équipements à votre disposition

4 TACHE 3 : PRESENTATION DE VOTRE OFFRE

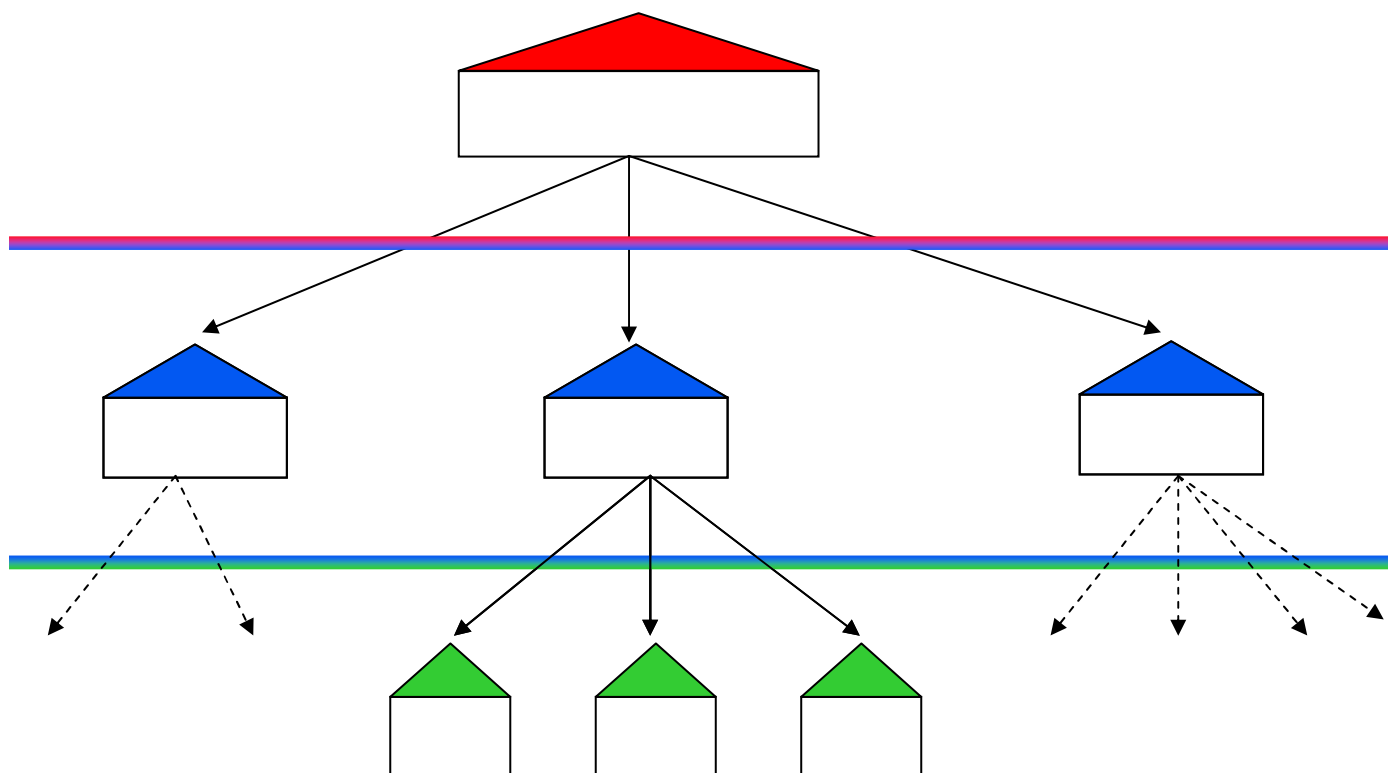
Il s'agit de présenter une synthèse de votre offre au client en définissant précisément

- Les choix retenus pour l'organisation de l'architecture applicative
- Les choix pour le déploiement
- L'organisation de votre infrastructure distribuée
- Démonstration de votre maquette et explication sur les points techniques demandés par le client.

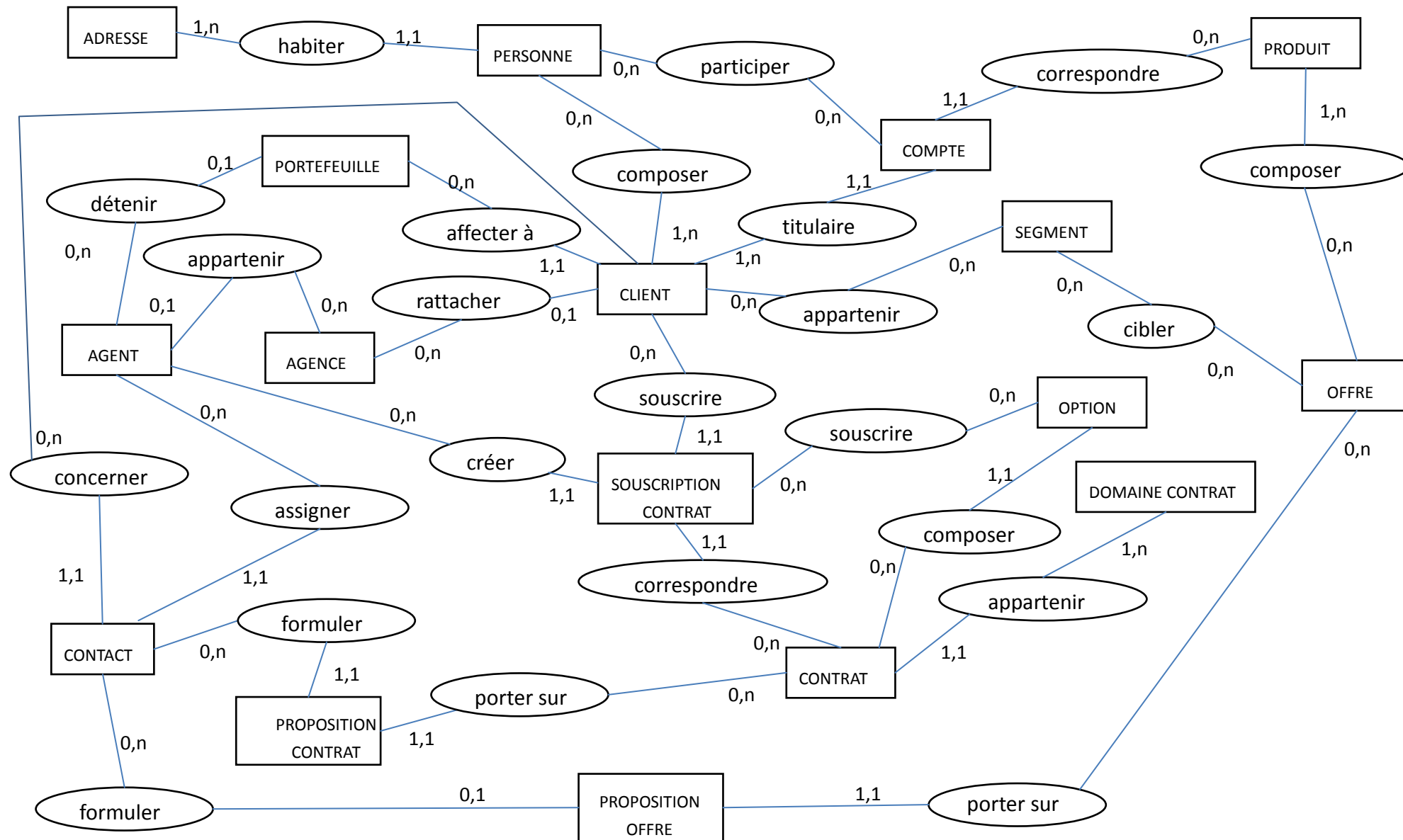
Annexes

5 DIAGRAMME D'ORGANISATION - MCD – CU

5.1 *DIAGRAMME D'ORGANISATION*



5.2 Modèle conceptuel de données – E-A



5.3 EXPRESSION DES BESOINS – SITUATIONS FONCTIONNELLES

Le dossier client a pour but de répondre aux différents besoins rencontrés face à un client: informations, connaissance, motifs de contact, historique... afin d'optimiser la gestion commerciale du client. Le dossier client est le support pour un agent lorsqu'il va préparer ou conduire un entretien, ou lorsqu'il veut consulter des informations sur un client. Le client a un numéro, une dénomination et une adresse postale principale.

5.3.1 CU1 – Consultation du dossier Client : Vue 360°

La vue synthétique du dossier client intitulée Vue 360° se décline de la façon suivante en 5 zones.

- **Zone Entête Client** : il s'agit des informations permettant de rapidement identifier le client.
- **Zone Client** : elle regroupe
 - la liste des personnes composant le client
 - des informations sur les cotations du client : ce sont des vues sur le risque, le potentiel, la réciprocité,
- **Zone Produits**: *il s'agit de la synthèse de ce que possède le client à la banque et à la concurrence, tant en terme de produits qu'en terme de services,*
- **Zone Contrats**: il s'agit de la synthèse des contrats que possède le client à la banque, selon les domaines (assurances, téléphonie mobile, santé, surveillance).
- **Zone relation banque/client** : elle regroupe les informations intéressant l'agent dans ses relations avec le client : les techniques de contact à privilégier ou à éviter, l'historique de l'ensemble des interactions avec le clients (contacts passés et à venir), *incidents antérieurs, événements à venir, réclamations faites par le client.*

5.3.2 CU2 – Gestion du client (Zone Client)

L'agent voudra consulter la liste des personnes composant le client et les informations spécifiques par personne.

Les données signalétiques d'une personne concernent la situation familiale, les revenus, les charges, la profession, la fiscalité, le logement.

Lors de l'évolution des informations liées à un client (obtenues lors d'un entretien par exemple), l'agent peut mettre à jour la liste des personnes d'un client. Il peut également en profiter pour actualiser les informations spécifiques d'une personne.

Afin de suivre l'évolution des informations sur les personnes, la date de dernière modification des informations d'une personne ainsi que le nom de l'agent ayant réalisé ces modifications, sont mémorisés et communiqués aux utilisateurs.

5.3.3 CU3 – Gestion des contacts clients (Zone Relation Banque/Client)

L'agent voudra consulter la liste des contacts du client. Il peut s'agir d'un **contact commercial** ou d'un **contact spontané** ou encore d'un **entretien**.

- Un contact commercial est pris par un agent avec un client par téléphone, mail ou autre selon les préférences du client.
- Lorsque le client prend contact de lui-même avec la banque, on parle de contact spontané, par téléphone, mail, courrier ou sur site.
- L'entretien correspond à une prise de rendez-vous entre le client et un agent suite à un contact spontané, contact commercial ou entretien précédent (appelé « contact origine » de cet entretien).

Un contact a toujours un motif et une date.

En fonction des interactions avec le client, des contacts sont créés ou mis à jour par les agents (motif, date, annotations...).

Au cours de la réalisation d'un entretien, l'agent a la possibilité de faire une ou des propositions sur les offres de produits du catalogue ou sur les offres de contrats, et d'ajouter des annotations. Lorsque l'entretien est terminé, l'agent clôture le contact.

Etats d'un contact : planifié, réalisé, annulé.

5.3.4 CU4 – Gestion des contrats du client (Zone Contrats)

L'agent voudra consulter la liste des contrats souscrits par le client dans chaque domaine.

Un contrat a un code contrat, un intitulé, un descriptif, et un tarif de base.

Un contrat peut proposer des options (payantes ou gratuites), qui sont par définition optionnelles et donc souscrites ou résiliées au fil du temps.

Selon les options choisies par le client, un tarif annuel est défini pour le contrat souscrit (numéro de contrat, date de souscription).

Suite à la périodicité de paiement choisie par le client, une mensualité est établie.

L'origine de la souscription au contrat (date et agent) est mémorisée et communiquée aux utilisateurs.

Un client peut mettre fin à son contrat en le résiliant.

Etats de souscription à une option : souscrite, non souscrite

6 DETAILS PRATIQUES POUR LA MISE EN ŒUVRE DU POC

6.1 CABLAGE DE VOTRE BANC

Vous disposez de

- 4 postes de travail sous Linux (Banc x - Machine 1 à Banc x – Machine 4) non connectées au réseau de production INSA
- 1 poste sous Windows connecté au réseau de production INSA vous permettant d'accéder à Internet
- 1 switch par hexanome
- 1 routeur matériel pour lequel vous aurez en charge la gestion des sauvegardes de vos configurations)
- 1 set de câblage

Vous êtes responsables de vos sauvegardes sur la plateforme

Attention : vos machines Linux sont équipées de 2 cartes réseaux. Les hexanomes des groupes 1 et 3 pourront accéder à la carte principale eml (noté ETH0 sur les câbles) alors que les hexanomes des groupes 2 et 4 accèderont à la carte additionnelle p255p1 (notée ETH1 sur les câbles).

Pour éviter les problèmes de « casse » et d'erreur de connexion sur les machines

- ➔ **Chaque machine est accessible par un câble RJ45 portant le numéro de la machine et le numéro de la carte**
- ➔ **Ne surtout pas rebrancher la connexion au réseau de production INSA**
- ➔ **Utiliser l'interrupteur de votre prise multiple pour éteindre les sonics et les switches de votre banc**

Votre set de câblage contient les câbles suffisants pour vous connecter au réseau d'interconnexion de la salle et connecter votre routeur. En cas de casse d'un câble, le remplacer et nous le signaler

6.2 PETITS DETAILS PRATIQUES

Où se trouve VirtualBox

Dans le menu système

Comment ajouter une machine à VirtualBox

Ouvrir un terminal et taper la commande : `/VMs/nom_de_la_VM/launch.sh`

Comment re-initialiser une VM que vous avez déjà ajoutée à VirtualBox

Ouvrir un terminal

Effacer les répertoires /home/hxxx/machines_virtuelles et
/home/.config/VirtualBox

Taper la commande : /VMs/nom_de_la_VM/launch.sh

Quel « manpage » lire de toute urgence

vconfig et ifconfig

Où trouver (un peu) de documentation

Sonic : Getting started guide:
Sonic : Administrator guide:
[http://www.sonicwall.com/app/projects/file_downloader/document lib.php?t=PG&id=142](http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=142)

Vyos : http://wiki.vyos.net/wiki/User_Guide

Quels sont les mots de passe

Machine physique linux

user : hexanome mot de passe : tpinfra

exemple user h4315 mot de passe tpinfra

VM Linux

root/TP4if2012

Simulateur pour les DAB et GAB

root/tpinfra

SonicWall

admin/password

Switch :

admin/pas de mot de passe (SVP ne pas modifier)

Serveur Windows

Administrator/TP4if2012

Centreon

admin/TP4if2012

Accès au switch:

adresse 192.168.168.169

Ne surtout pas changer son adresse par défaut

Machines Debian

Root / mars

Admin Tomcat

accès http://<IP>:8080/manager

tomcat/pwd-tomcat-admin

Admin BD MySQL

accès http://<IP>/phpmyadmin

root/pwd-mysql-root

Admin LDAP

accès http://<IP>/phpldapadmin

cn=admin, dc=mars / pwd-ldap-admin

Comment accéder à la configuration du routeur Vynos pour le premier lancement (rétablir les adresses MAC) : Le mode de mise en production par clonage des machines en retirant les adresses MAC impose de modifier manuellement le fichier de configuration construit par Vynos. Quand vous faites un launch de l'un des routeurs Vynos, vous devez

- Noter les adresses MAC associées aux cartes Eth0 à ETHx sur Virtual Box
- Editer le fichier /config/config.boot pour détruire les lignes décrivant les interfaces avec les mauvaises MAC et renuméroter les dernières lignes (de 0 à 2 ou à 3 selon le Vynos traité et son nombre de cartes) pour les Poaffecter aux interfaces ETH0 à ETHx

Pour configurer le switch : il y a un risque d'accès aux switch d'autres hexanomes lorsque vous accédez au 192.168.168.169 et que votre switch est connecté à l'interco. Pour y remédier :

- o Soit vous faites des accès pour configurer le switch UNIQUEMENT lorsque celui n'est pas connecté sur l'interconnexion.
- o Soit vous limitez les ports dédiés au VLAN par défaut (VLAN1) au strict nécessaire. Par exemple vous pouvez conserver un port non taggé vous permettant de vous connecter directement au switch sans créer de VLAN

sur la machine qui y sera raccordée et / ou dédier un port pour la configuration en le TAGGANT sur le VLAN par défaut (VLAN 1).

Accès au sonic : Adresse 192.168.168.168

Reset des sonicwall : Appuyer longuement sur le bouton reset (voyant clignote) puis se connecter en http et le rebooter en factory default

Adresse du DNS de la salle (racine tp4if) : 10.0.10.1

6.3 AFFECTATION DES ADRESSES IP PAR HEXANOME

	IP Unique	IP Unique	Paires IP		Paires IP	
Hexanome	IP1	IP2	IP3	IP4	IP5	IP6
4101	10.0.9.17	10.0.9.52	10.0.9.34	10.0.9.35	10.0.9.1	10.0.9.2
4102	10.0.9.49	10.0.9.84	10.0.9.68	10.0.9.69	10.0.9.9	10.0.9.10
4103	10.0.9.81	10.0.9.116	10.0.9.100	10.0.9.101	10.0.9.65	10.0.9.66
4104	10.0.9.113	10.0.9.6	10.0.9.132	10.0.9.133	10.0.9.97	10.0.9.98
4105	10.0.9.3	10.0.9.36	10.0.9.21	10.0.9.22	10.0.9.129	10.0.9.130
4201	10.0.9.33	10.0.9.70	10.0.9.53	10.0.9.54	10.0.9.18	10.0.9.19
4202	10.0.9.67	10.0.9.102	10.0.9.85	10.0.9.86	10.0.9.50	10.0.9.51
4203	10.0.9.99	10.0.9.134	10.0.9.117	10.0.9.118	10.0.9.82	10.0.9.83
4204	10.0.9.131	10.0.9.23	10.0.9.7	10.0.9.8	10.0.9.114	10.0.9.115
4205	10.0.9.20	10.0.9.55	10.0.9.37	10.0.9.38	10.0.9.4	10.0.9.5
4301	10.0.9.17	10.0.9.52	10.0.9.34	10.0.9.35	10.0.9.1	10.0.9.2
4302	10.0.9.49	10.0.9.84	10.0.9.68	10.0.9.69	10.0.9.9	10.0.9.10
4303	10.0.9.81	10.0.9.116	10.0.9.100	10.0.9.101	10.0.9.65	10.0.9.66
4304	10.0.9.113	10.0.9.6	10.0.9.132	10.0.9.133	10.0.9.97	10.0.9.98
4305	10.0.9.3	10.0.9.36	10.0.9.21	10.0.9.22	10.0.9.129	10.0.9.130
4401	10.0.9.33	10.0.9.70	10.0.9.53	10.0.9.54	10.0.9.18	10.0.9.19
4402	10.0.9.67	10.0.9.102	10.0.9.85	10.0.9.86	10.0.9.50	10.0.9.51
4403	10.0.9.99	10.0.9.134	10.0.9.117	10.0.9.118	10.0.9.82	10.0.9.83
4404	10.0.9.131	10.0.9.23	10.0.9.7	10.0.9.8	10.0.9.114	10.0.9.115
4405	10.0.9.20	10.0.9.55	10.0.9.37	10.0.9.38	10.0.9.4	10.0.9.5

6.4 AFFECTATION DES RESEAUX AUX PORTS DES SWITCH D'INTERCONNEXION, ADRESSES DES ROUTEURS ET MASQUE DE RESEAU

Réseau	Masque	Adresse Routeur	Port sur les switch
10.0.10.0	24	1	Vlan 9 sur (19,20) et (21,22)
10.0.9.0	28	14	1,2
10.0.9.16	28	30	3,4
10.0.9.32	28	46	5,6
10.0.9.48	28	62	7,8
10.0.9.64	28	78	9, 10
10.0.9.80	28	94	11,12
10.0.9.96	28	110	13,14
10.0.9.112	28	126	15,16
10.0.9.128	28	142	17,18

Les parenthèses entourant deux numéros de ports signifient que ceux-ci sont agrégés et vus comme un seul.

6.5 CATALOGUE DE MACHINE VIRTUELLE

Machine	Mémoire	OS	Fonction
DAB-Site1-1	512	Linux	Simulateur Automate
DAB-Site1-2	512	Linux	Simulateur Automate
DAB-Site2-1	512	Linux	Simulateur Automate
DAB-Site2-2	512	Linux	Simulateur Automate
DAB-Site3-1	512	Linux	Simulateur Automate
DAB-Site3-2	512	Linux	Simulateur Automate
PC-Site-1-1	512	Windows 7	poste client
PC-Site-1-2	512	Windows 7	poste client
PC-Site-2-1	512	Windows 7	poste client
PC-Site-2-2	512	Windows 7	poste client
PC-Site-3-1	512	Windows 7	poste client
PC-Site-3-2	512	Windows 7	poste client
PC-Site-4-1	512	Windows 7	poste client
Machine	Mémoire	OS	Fonction

PC-Site-4-2	512	Windows 7	poste client
Portable-nomade	512	Windows 7	poste client
Lin-centreon-1	512	CentOs	Supervision Centreon + DNS +DHCP
Lin-centreon-2	512	CentOs	Supervision Centreon + DNS +DHCP
Win-DNS-DHCP-1	512	Windows 2008 server	DNS+DHCP
Win-DNS-DHCP-2	512	Windows 2008 server	DNS+DHCP
Lin-Proxy	512	CentOs	Apache
Lin-wrksta	512	CentOS	poste client
PLD-MARS-Debian.lldap	512	Debian	Annuaire Ldap
PLD-MARS-Debian.web1	512	Debian	Serveur d'application Tomcat+ Serveur Apache+ BDMysql
PLD-MARS-Debian.web2	512	Debian	Serveur d'application Tomcat+ Serveur Apache+ BDMysql
PLD-MARS-Debian.web3	512	Debian	Serveur d'application Tomcat+ Serveur Apache+ BDMysql
Vyos-Agence-Principale1	512	Vyos	Routeur virtualisé Vyos
Vyos-Agence-Principale2	512	Vyos	Routeur virtualisé Vyos
Vyos-Agence-Secondaire	512	Vyos	Routeur virtualisé Vyos

6.6 LIVRABLES ATTENDUS

Présentation de l'architecture détaillée (au cours de la séance 1) : vous devez nous fournir un schéma détaillé montrant votre plan d'adressage et les éléments principaux de configuration des machines et équipements ainsi qu'un plan de câblage et le principe de nommage retenu.

Démonstration / validation des différents éléments de la solution au fil de l'eau

L'évaluation finale est réalisée lors d'une présentation / démonstration réalisée pour le client lors de la dernière séance du PLD en intégrant la présentation de votre architecture logicielle.

7 CAHIER DE TP : MEMENTO SUR LES ETAPES A SUIVRE

Hexanome :

Groupe

Noms :

Validation specifications :

Validation finale : Le _____ à _____

Validation :

Date :
validée

Enseignant :

Partie

7.1 CONCEPTION DE L'ARCHITECTURE

7.1.1 Organisation du plan d'adressage

Contrairement aux exercices de 3lfs, vous n'avez pas de contraintes d'espace limité.

Combien de sous-réseaux avez-vous pour le site du siège

A quoi sert chaque sous-réseau

Combien de sous-réseaux avez-vous pour le site d'une agence principale

A quoi sert chaque sous-réseau

Combien de sous-réseaux avez-vous pour le site d'une agence secondaire

A quoi sert chaque sous-réseau

Organiser un plan (adresse réseau et masque) qui vous permette d'identifier facilement les 4 sites puis les sous-réseaux de chaque site

Qu'est ce qui permet de résumer l'accès au site du siège (adresse et masque)

Qu'est ce qui permet de résumer l'accès au site de l'agence principale 1 (adresse et masque)

Qu'est ce qui permet de résumer l'accès au site de l'agence secondaire (adresse et masque)

Qu'est ce qui permet de résumer l'accès au site de l'agence principale 2 (adresse et masque)

7.1.2 Organisation de l'architecture globale

Quel type d'équipement permet de connecter une machine sur un réseau

Comment pouvez-vous relier le site du siège au site d'une agence de manière sécurisée

Comment pouvez-vous relier le site de l'agence secondaire au site de l'agence principale 1 de manière sécurisée

Donner le schéma global en précisant les éléments du plan d'adressage

7.1.3 Organisation du POC sur table

Sachant que le switch et le routeur ont des adresses d'administration en 192.168.168.168 et 192.168.168.169, que devez-vous configurer pour y accéder à partir de l'une des machines

Comment éviter d'accéder au switch d'un autre groupe une fois relié au réseau d'interconnexion ?

Comment répartir les différentes VM sur les 4 machines à votre disposition (quelles sont les contraintes à prendre en compte)

Peut-on séparer les flux issus des différentes VM sur le switch à votre disposition ?

Expliquer comment

Dessinez le plan de câblage en indiquant les VM tournant sur chaque machine, positionnez les interfaces des boitiers Sonic et indiquer les paramètres de configuration pour chaque port du switch

7.1.4 Maîtrise de la chaîne de liaison

Expliquer le cheminement des paquets

➔ Entre un poste du réseau automate et un poste du réseau gestion du site d'une agence

➔ Entre un poste du réseau gestion du siège et un serveur

➔ Entre un poste de travail de l'agence secondaire se connectant au serveur de son agence de référence

➔ Entre un poste de travail de l'agence principale se connectant au serveur du siège

7.1.5 Organisation de l'espace de nommage (facultatif)

Quelle est votre arborescence de nommage

Quelle(s) machine(s) héberge(nt) le(s) annuaire(s) associé(s) à quelle partie de l'arborescence

Comment assurer la continuité de service en cas de panne d'un serveur de nom

7.2 PREPARATION DE VOTRE BANC

Utilisez votre plan de câblage et les documents de la première séance. Pensez à bien sauvegarder vos fichiers de configuration

Il faut mettre en place vos chaînes de liaison étape par étape. Assurez-vous des résultats avant de poursuivre. Reprenez les explications des différents cheminements et précisez-les au fur et à mesure de votre avancée.

7.2.1 Configuration de vos machines

Quelle commande utilisez-vous pour créer des cartes virtuelles

Quelle(s) commande(s) permettent de paramétrer l'interface IP d'une machine sous Linux

Comment paramétrer l'interface IP d'une machine sous Windows

Expliquer le chemin d'un paquet sur la machine virtuelle jusqu'à l'interface de sortie et définir comment et où configurer les paramètres réseau

7.2.2 Configuration de votre switch

Définissez la configuration des différents ports à partir de votre organisation en VLAN et de votre plan de câblage.

Testez la connexion entre 2 machines d'un même sous-réseau grâce à un ping

Test	Passe	Ne passe pas
Ping entre 2 machines du réseau de gestion du siège		
Ping entre 2 machines du réseau serveur du siège		
Ping entre 2 machines du réseau de gestion de l'agence principale 1		
Ping entre 2 machines du réseau automate de l'agence principale 1		
Ping entre 2 machines du réseau serveur de l'agence principale 1		
Ping entre 2 machines du réseau serveur de l'agence principale 2		
Ping entre 2 machines du réseau de gestion de l'agence secondaire		
Ping entre 2 machines du réseau automate du site de l'agence secondaire		
Ping entre 2 machines du réseau de gestion de l'agence principale 2		
Ping entre 2 machines du réseau automate de l'agence principale 2		

7.2.3 Configuration de vos routeurs

Rappelez les éléments de configuration de chaque port (adresse, masque, VLAN...)

Expliquer la configuration des ports du switch pour y raccorder ces ports de routeur :
quelle est la différence avec la connexion de l'une de vos machines physiques ?

7.2.4 Configuration des connexions sur un même site

Routeur du siège :

Configurez le routeur du siège pour permettre à 2 machines de sous-réseaux différents de communiquer. ATTENTION : il faut aussi autoriser les ping !

Test	Passe	Ne passe pas
Ping depuis le routeur vers une machine du réseau de gestion		
Ping depuis le routeur vers une machine du réseau automates		
Ping depuis le routeur vers une machine de la zone serveur		
Ping depuis 1 machine du réseau de gestion vers le réseau automate		
Ping depuis 1 machine du réseau automate vers le réseau de gestion		
Ping depuis 1 machine du réseau de gestion vers le réseau serveur		
Ping depuis le réseau serveur vers une machine du réseau de gestion		

Routeur de l'agence principale 1:

Configurez le routeur Vyos de l'agence principale 1 pour permettre à 2 machines de sous-réseaux différents de communiquer. ATTENTION : il faut aussi autoriser les ping !

Test	Passe	Ne passe pas
Ping depuis le routeur vers une machine du réseau de gestion		
Ping depuis le routeur vers une machine du réseau automates		
Ping depuis le routeur vers une machine de la zone serveur		
Ping depuis 1 machine du réseau de gestion vers le réseau automate		
Ping depuis 1 machine du réseau automate vers le réseau de gestion		
Ping depuis 1 machine du réseau de gestion vers le réseau serveur		
Ping depuis le réseau serveur vers une machine du réseau de gestion		

Routeur de l'agence principale 2:

Configurez le routeur Vyos de l'agence principale 2 pour permettre à 2 machines de sous-réseaux différents de communiquer. ATTENTION : il faut aussi autoriser les ping !

Test	Passe	Ne passe pas
Ping depuis le routeur vers une machine du réseau de gestion		
Ping depuis le routeur vers une machine du réseau automates		
Ping depuis le routeur vers une machine de la zone serveur		
Ping depuis 1 machine du réseau de gestion vers le réseau automate		
Ping depuis 1 machine du réseau automate vers le réseau de gestion		

Test	Passe	Ne passe pas
Ping depuis 1 machine du réseau de gestion vers le réseau serveur		
Ping depuis le réseau serveur vers une machine du réseau de gestion		

Routeur de l'agence secondaire:

Configurez le routeur Vynos de l'agence secondaire pour permettre à 2 machines de sous-réseaux différents de communiquer. ATTENTION : il faut aussi autoriser les ping !

Test	Passe	Ne passe pas
Ping depuis le routeur vers une machine du réseau de gestion		
Ping depuis le routeur vers une machine du réseau automates		
Ping depuis 1 machine du réseau de gestion vers le réseau automate		
Ping depuis 1 machine du réseau automate vers le réseau de gestion		

Paramétrage des routeurs pour réaliser l'interconnexion des sites

Construisez ensuite le VPN entre sites et vérifiez qu'une machine du site central peut pinger une machine du site distant.

- ➔ Quelles sont les adresses des extrémités du tunnel
- ➔ Comment les routeurs vont-ils s'authentifier ?
- ➔ Comment est gérée la confidentialité de l'échange ?
- ➔ Quelle est la chaîne de liaison exacte lorsqu'on fait un ping entre une machine du siège et d'une agence

Test	Passe	Ne passe pas
Ping depuis le routeur du site central vers le routeur du site distant		
Ping depuis une machine du réseau automate du siège vers une machine du réseau automate d'une agence		
Ping depuis 1 machine du réseau de gestion du siège vers le réseau automate d'une agence		
Ping depuis 1 machine du réseau de gestion du siège vers une machine du réseau de gestion de l'agence		
Ping depuis une machine du réseau automate du siège vers une machine du réseau de gestion de l'agence		

7.3 MISE EN PLACE D'ACCES EXTERNES POUR LE TELETRAVAIL: VPN SSL

- ➔ Quelles seront les extrémités du tunnel ?
- ➔ Comment sera connecté le poste client de test (VLAN, adressage...)
- ➔ Que doit-on configurer pour activer ce VPN (droits)
- ➔ Montrer qu'un poste extérieur peut accéder à une ressource interne
- ➔ Expliquer la chaîne de liaison

7.4 GESTION DES CONFIGURATIONS

7.4.1 Organisation du DHCP

- Est-ce que toutes les machines doivent être configurées en DHCP ? quel est l'intérêt, quelles sont les limites ?

Configuration sur le siège

- Combien d'étendues devez-vous gérer

- Pour chaque étendue identifiez les paramètres de configuration (@réseau, masque, @passerelle, ...)

- Comment définir les adresses à distribuer ? Comment donner une adresse fixe à une machine particulière ?

- Comment le serveur peut-il savoir à quelle étendue est associée la demande ?

- quels fichiers doivent être mis à jour

- ➔ Comment lancer le serveur ?

- ➔ Faire un test d'allocation d'adresse pour une machine sur le même sous-réseau que le serveur DHCP

- ➔ Que doit-on modifier sur le routeur pour que le serveur puisse donner des adresses aux machines de l'autre sous-réseau ?

- ➔ Faites un test d'allocation d'adresse pour une machine de l'autre sous-réseau.

Configuration sur le site d'une agence

- ➔ Combien d'étendues devez-vous gérer

- ➔ Pour chaque étendue identifiez les paramètres de configuration (@réseau, masque, @passerelle, ...)

- ➔ Comment définir les adresses à distribuer ? Comment donner une adresse fixe à une machine particulière ?

→ Comment lancer le serveur DHCP du routeur

→ Listez les éléments de configuration paramétrés pour le serveur DHCP du site

7.4.2 Organisation du DNS (facultatif)

→ Rappeler votre arbre de nommage

→ Quel est le serveur de référence pour chaque espace

→ Quels sont les serveurs associés à chaque zone

→ Quelles sont les informations à nous transmettre pour demander la délégation sur votre zone

Configuration du serveur

- ➔ Identifiez les fichiers à créer / mettre à jour

- ➔ Comment lancer ce service de nommage

- ➔ Quels sont les enregistrements à créer pour dire qui gère un espace de nommage ?

- ➔ Créer l'enregistrement permettant de trouver le nom de quelques machines

- ➔ Essayer de faire un ping sur les machines à partir de leur nom

Si vous mettez une réplication : configuration du serveur sur une agence

- ➔ Comment lancer ce service de nommage

- ➔ Quels sont les paramètres de configuration par type d'enregistrement
 - SOA

 - NS

 - A

 - PTR

➔ Essayer de faire un ping sur les machines à partir de leur nom

Accès depuis l'extérieur et gestion de la réplication

➔ Comment peut-on accéder au DNS depuis l'extérieur ? Quel équipement doit-on paramétrer ?

➔ Comment lier vos serveurs pour assurer une reprise ?

➔ Testez