

SAÉ 3.01 : Mettre en œuvre un système de transmission
SAÉ 3.02 : Déployer un réseau multi-sites

Cahier des charges



Table des matières

I) Introduction.....	3
1) Contexte du projet.....	3
2) Lots techniques - généralités.....	4
2.1) Lot Infrastructure, LAN et WAN.....	4
2.2) Lot Système et Services.....	4
II) Détail des lots – cahier des charges complet.....	5
1) Lot Infra LAN/WAN.....	5
Plan IP.....	5
Sécurisation des services et échanges.....	5
OSPF.....	5
Boucle fibre optique.....	5
VPN.....	6
VLAN.....	6
Wi-Fi.....	6
2) Lot Système et Services.....	6
Virtualisation.....	6
Stockage.....	7
Annuaire.....	7
Travail collaboratif.....	7
Résolution de noms.....	7
Distribution d’adresses et référence de temps.....	7
Téléphonie.....	7
III) Évaluation.....	8
1) Généralités.....	8
2) Détail des évaluations.....	8
Suivi hebdomadaire.....	8
Oral de groupe final.....	8
Oral individuel.....	8
Livrables techniques.....	9
QCM.....	9
Annexe : tableau synthétique des lots.....	9

I) Introduction

Réseau local, Wi-Fi, VPN, backbone, annuaire LDAP, hyperviseur Proxmox, ... Autant de mots qui font régulièrement partie du volet télécommunication d'une entreprise moderne. Il est important de comprendre les principaux enjeux théoriques, mais la manipulation avec une approche de bout-en-bout, est une étape primordiale.

A travers un ensemble de manipulations, vous allez devoir contribuer à la mise en œuvre d'un véritable scénario pour lequel, par groupes, vous serez responsables d'un volet technique complet.

1) Contexte du projet



PolyLED est un acteur montant de l'éclairage à base de semi-conducteurs.

Il s'agit d'une entreprise française répartie sur différents sites :

- Le siège social de l'entreprise est basé à Caen, c'est aussi sur ce site que l'ensemble des briques indispensables au système d'information est stocké. Il compte environ 150 postes utilisateurs.
- Une usine de production est basée à Lyon, elle dispose de postes utilisateurs et d'automates pour la chaîne de production. Ce site compte environ 200 postes.
- De plus, de nombreux chargés d'affaires sont mobiles et nécessitent un accès au SI à distance afin d'effectuer du télé-travail.

Le conseil d'administration de PolyLED n'étant pas satisfait de son ancien opérateur, il a choisi la société **Krypcom**, opérateur international de télécommunications pour la réalisation de l'ensemble de ses besoins en communication ainsi qu'un volet d'infogérance.

Votre mission en tant que collaborateurs de l'entreprise Krypcom : délivrer un service télécoms à valeur ajoutée à l'entreprise PolyLED et ses sous-traitants. L'ensemble du parc informatique de PolyLED possède de postes sous Ubuntu 22.04.1 LTS. En conséquence, vous devrez déployer des solutions gratuites et compatibles avec les distributions GNU/Linux.

Vous devrez mettre en œuvre une solution technique répondant aux besoins définis dans le cahier des charges. Ce cahier des charges a été établi par les chefs de projet en étroite collaboration avec le client final et contient la liste des détails techniques attendus.

A l'issue de la mise en œuvre de l'offre de prestation, une démonstration est programmée, qui doit permettre à chaque groupe d'illustrer son travail et de montrer l'apport dans la solution globale, mais également la restitution des problèmes rencontrés, les alternatives techniques utilisées, etc.

2) Lots techniques - généralités

Le cahier des charges est découpé selon deux grandes catégories qui sont des lots techniques de thématique différentes. Il s'agit d'un découpage logique pour comprendre l'ensemble des besoins mais aussi du nom des équipes de travail qui seront constituées chez Krypcom.

Attention : même si chaque étudiant a une ou plusieurs tâches affectées au long du projet, cela ne veut pas dire que chacun travaille en autonomie dans son coin. Vous avez comme responsabilité d'avoir une vue d'ensemble du projet et de comprendre les différentes briques techniques. Les groupes ne sont pas figés dans le temps, si vous avez terminé « votre partie » il est important de redistribuer le travail et de modifier les assignations.

2.1) Lot Infrastructure, LAN et WAN

Ce volet représente l'ensemble des technologies qui vont permettre l'interconnexion au niveau physique et logique des différents sites de l'entreprise PolyLED. Il s'agit donc à la fois du déploiement réseau du point de vue WAN (entre les différents sites et l'Internet) et du point de vue LAN (au sein de chaque site)

Mots-clés : routage OSPF, boucle fibre entre sites distants, switching, VLAN, Wi-Fi, VPN inter-site et VPN nomade

2.2) Lot Système et Services

Ce volet regroupe les différents serveurs nécessaires au bon fonctionnement du système d'information et des applications client. Il s'agit de services transparents pour l'utilisateur lambda sur lesquels vont s'appuyer les applications finales utilisées par les employés de PolyLED.

Mots-clés : LDAP, DNS, DHCP et NTP, NAS, hyperviseur Proxmox, IPBX, Nextcloud, WebDAV

II) Détail des lots – cahier des charges complet

1) Lot Infra LAN/WAN

Les sites de Caen et Lyon pour le client PolyLED sont interconnectés au sein du cœur de réseau opérateur Krypcom. Celui-ci est commun à plusieurs clients de l'opérateur, c'est pourquoi plusieurs préconisations sont à prendre afin d'isoler le trafic entre les différents clients.

Plan IP

Les routeurs en charge de l'interconnexion des sites sur le backbone doivent être configurés avec des adresses IPv4 publiques. Pour chaque site client, on définira un plan IP logique privé, dimensionné aux besoins de l'entreprise et qui prendra en compte les évolutions futures du système d'information.

Sécurisation des services et échanges

Dans un souci de sécurisation des trafics, les sites client devront implémenter une architecture de type « zone démilitarisée » (DMZ) avec à disposition des pare-feu série 110 Fortigate. L'ensemble des services de l'entreprise est hébergé sur l'hyperviseur du site de Caen.

Sur chaque site, les différents services de l'entreprise seront isolés les uns des autres et devront communiquer ensemble selon les besoins. On mettra alors en place du filtrage par ACL sur les routeurs internes.

OSPF

D'un point de vue logique :

- le routage est effectué via le protocole OSPF
- l'ensemble des routeurs OSPF ne doit pas être dans la même zone, un découpage logique avec une zone backbone d'aire zéro et d'autres aires doit être étudié et mis en place
- la route par défaut vers l'Internet est simulée via les Box Orange à disposition en salle serveur, cette route doit être redistribuée au travers du routage OSPF (attention pendant les séances de projet à utiliser intelligemment les Box, si vous êtes à 20 sur une ADSL cela va poser problème)

Boucle fibre optique

D'un point de vue physique :

- une boucle de fibre optique permet d'interconnecter les différents clients de l'opérateur Krypcom, parmi ces clients se trouve PolyLED mais ce n'est pas le seul !
- vous implémenterez une boucle CWDM avec le matériel à disposition à l'IUT
- chaque site client utilise une longueur d'onde différente

VPN

Les échanges entre le site de Caen et de Lyon doivent être chiffrés et le réseau local étendu à l'aide d'un VPN IPSec. Les choix des algorithmes cryptographiques et autres paramètres de sécurité doivent respecter les dernières préconisations de l'ANSSI.

Un accès VPN nomade doit être à disposition pour les employés de PolyLED effectuant du télé-travail. Celui-ci permettra l'accès à toutes les applications client de l'entreprise comme s'il était sur site, mais encore une fois dans le respect des préconisations de l'ANSSI. L'authentification des utilisateurs sera basée sur l'annuaire LDAP de l'entreprise.

Pour l'implémentation, les tunnels seront montés entre les pare-feu disponibles sur chaque site.

VLAN

Un découpage logique de niveau 2 doit être mis en place afin de différencier les utilisateurs classiques du système d'information (VLAN « production ») et les administrateurs réseau de l'entreprise PolyLED (VLAN « admin »)

Les administrateurs de l'entreprise doivent pouvoir intervenir sur toutes les machines à l'aide de routage inter-VLAN.

Wi-Fi

Sur le site de Lyon, certains automates de l'usine de production ne possèdent pas d'interfaces Ethernet filaire et nécessitent donc un accès Wi-Fi. Il faut donc couvrir le site de Lyon en Wi-Fi 802.11n en 5Ghz, l'authentification sera basée sur un serveur RADIUS interfacé avec l'annuaire LDAP de l'entreprise pour les comptes utilisateurs.

2) Lot Système et Services

Virtualisation

Un hyperviseur sous la solution Proxmox doit être déployé sur le site de Caen afin d'héberger toutes les machines virtuelles nécessaires pour les différents serveurs de l'entreprise.

- fonctionnement en mode «cluster» avec un minimum de 3 nœuds
- stockage des machines virtuelles sur un NAS dédié
- en cas de perte d'un des serveurs hôtes, les VM qu'il héberge doivent être redémarrées sur un autre hôte (principe de haute-disponibilité)
- possibilité de migration à chaud des VM
- gestion automatique des sauvegardes
- gestion des utilisateurs du Proxmox pour que chacun gère ses machines virtuelles

Attention : c'est une brique technique essentielle au bon déroulement du projet ! Réfléchissez bien à sa mise en place et à votre politique de sauvegarde des machines virtuelles

Stockage

L'entreprise PolyLED nécessite deux serveurs NAS pour deux usages différents :

- le premier a pour but de contenir les machines virtuelles hébergées sur l'hyperviseur Proxmox
- le deuxième contient toutes les données personnelles des utilisateurs (répertoires « home ») et d'autres partages de fichiers communs à plusieurs utilisateurs (Nextcloud)

La solution NAS devra utiliser des disques avec une grappe RAID adaptée aux besoins.

Annuaire

Un service LDAP doit référencer la liste des utilisateurs de l'entreprise PolyLED. On pensera à déclarer des Unités Organisationnelles afin de différencier plusieurs types d'utilisateurs (par exemple : Direction, Production, Administrateurs)

Travail collaboratif

Une solution Nextcloud est à disposition des utilisateurs de PolyLED pour :

- accéder depuis un client Web à leurs fichiers personnels et autres partages
- permettre le partage de fichiers entre utilisateurs avec gestion des droits
- utiliser des outils de travail collaboratif pour éditer des documents texte ou des tableurs en simultané avec gestion des accès concurrents (OnlyOffice ou CollaboraOnline)

La solution Nextcloud devra être interfacée avec l'annuaire LDAP pour la gestion des utilisateurs, par la suite il faudra effectuer un montage automatique sur le réseau des répertoires personnels des utilisateurs à l'ouverture de la session.

Résolution de noms

L'entreprise PolyLED possède son propre nom de domaine et héberge son serveur DNS.

- les serveurs DNS sont utilisés pour la résolution de noms en interne et noms externe
- tous les serveurs internes à l'entreprise doivent être référencés dans le DNS
- afin de minimiser le trafic, les DNS devront faire office de cache pour ne pas sortir du Backbone lors d'une résolution de nom déjà connu

Distribution d'adresses et référence de temps

Un serveur DHCP doit être déployé sur le site de Caen afin de fournir des adresses IP aux différents postes clients du site. Sur le site de Lyon, on utilisera le routeur de sortie comme serveur DHCP. La configuration redescendue doit bien sûr comprendre tous les paramètres utiles pour le bon fonctionnement des postes (passerelle par défaut, etc)

Un serveur NTP fera office de référence de temps pour les machines de l'entreprise.

Téléphonie

Un serveur de téléphonie doit être déployé afin de permettre la communication entre les différents employés de l'entreprise. Le choix de la solution est libre mais doit être de la téléphonie basée sur IP et permettre l'utilisation de différents terminaux : téléphone filaire, DECT, Softphone sur PC.

III) Évaluation

1) Généralités

Le projet s'inscrit sur deux SAÉ et l'évaluation se fait sous plusieurs formes, voici le détail :

SAE3.01 : soutenances individuelles + QCM individuel

SAE3.02 : suivi hebdomadaire + oraux de groupe + livrables

Les coefficients seront probablement pondérés équitablement mais cela peut encore changer.

2) Détail des évaluations

Suivi hebdomadaire

A chaque fin de semaine, les chefs de groupe doivent rendre un rapport d'activité par mail. Celui-ci résume pour la semaine courante, lot par lot, les objectifs des séances de projet, le travail accompli, les difficultés rencontrées, les éléments à prioriser et éventuelles questions à remonter, le travail à effectuer à la séance d'après, etc.

Ce document a deux intérêts :

- permettre aux chefs de projet de suivre de l'extérieur l'avancement du projet
- vous forcer à vous organiser convenablement pour faire le point sur votre travail

Il devra être remis par mail au plus tard le Vendredi à 18h à M. Lepaulmier et M. Brisacier.

Même si ce sont les chefs de groupe qui font le rendu, tous les étudiants ont pour responsabilité de participer à sa rédaction et surtout tous ont pour obligation de le lire et d'être au courant de l'état actuel du projet.

NB : certaines questions du QCM final seront tirées de ces rapports d'activité

Oral de groupe final

A la fin du semestre, un oral par groupe de projet est prévu afin de restituer le travail. Vous devrez alors faire l'état d'avancement du projet par lot technique, expliquer les points de blocage et présenter des démonstrations techniques de votre travail pour prouver du bon fonctionnement des services demandés dans le cahier des charges.

Les modalités d'évaluation et de notation vous seront transmises ultérieurement.

Oral individuel

Après les oraux de groupe, chaque étudiant devra présenter devant un jury restreint son travail effectué pendant le semestre sur le projet. L'accent sera mis sur le retour d'expérience et des compétences acquises.

Les modalités d'évaluation et de notation vous seront transmises ultérieurement.

Livrables techniques

A la fin du projet, vous devrez rendre par lot plusieurs documents qui auront été réalisés tout au long de votre travail. Attention cette partie est à ne pas négliger !

- PTI : documentation d'installation d'un lot
 - PEE : documentation prouvant le bon fonctionnement d'un lot (recette)
 - DIO : documentation technique globale (schémas physiques et logiques, flux, ports utilisés, etc.)
- des modèles et explications vous seront fournis par M. Lepaulmier dans la Ressource 3.15

QCM

Toujours à la fin du projet, un QCM individuel aura lieu afin d'évaluer vos connaissances sur le projet. Il s'agira de questions générales sur les différents lots, leurs dépendances, les difficultés rencontrés, etc. Certaines questions pourront être tirées de vos expériences et des rapports d'activité, c'est pourquoi vous devez vous responsabiliser en ayant une vision globale du projet à tout moment.

Annexe : tableau synthétique des lots

Équipe Alpha – lot Infrastructure LAN/WAN	Équipe Bravo – lot Système et Services
Définition du plan IP	Hyperviseur Proxmox
Boucle fibre OADM	NAS stockage VM et NAS utilisateur
Routage backbone et LAN - OSPF	Annuaire LDAP
VPN inter-site, VPN nomade	Résolution DNS et attribution DHCP
Wi-Fi et Radius	Téléphonie sur IP (IBPX)
VLAN	Stockage Nextcloud et partage de fichiers