



**HAL**  
open science

# Conception et réalisation d'une solution de diffusion des flux pédagogiques multimédias de l'espace numérique de travail de l'École des transmissions

Michaël Blaublomme

## ► To cite this version:

Michaël Blaublomme. Conception et réalisation d'une solution de diffusion des flux pédagogiques multimédias de l'espace numérique de travail de l'École des transmissions. Architectures Matérielles [cs.AR]. 2011. dumas-00692471

**HAL Id: dumas-00692471**

**<https://dumas.ccsd.cnrs.fr/dumas-00692471>**

Submitted on 10 May 2012

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**CONSERVATOIRE NATIONAL DES ARTS ET METIERS**

**CENTRE REGIONAL ASSOCIE DE RENNES**

---

**MEMOIRE**

**présenté en vue d'obtenir**

**le diplôme D'INGENIEUR CNAM**

**SPECIALITE : Informatique**

**OPTION : Architecture et Ingénierie des Systèmes et des Logiciels**

**par**

**BLAUBLOMME Michaël**

---

Conception et réalisation d'une solution de diffusion  
des flux pédagogiques multimédias de  
l'espace numérique de travail de l'École des transmissions.

**Soutenu le 17 juin 2011**

---

**JURY**

**Président :**           **Professeur Yann POLLET**

**Membres :**           **Monsieur Éric BORNETTE**  
**Monsieur Thierry MARTINEAU**  
**Monsieur Patrick JAOUEN**  
**Monsieur Romuald LORTHIOIR**



Conception et réalisation d'une solution de diffusion des flux pédagogiques multimédias de l'espace numérique de travail de l'École des transmissions.

Mémoire d'ingénieur CNAM, Rennes 2011.

---

## RESUME

L'École des transmissions de Cesson-Sévigné est une école interarmées spécialisée dans la formation du personnel du ministère de la Défense dans le domaine des systèmes d'information et de communication et la guerre électronique. Dans un contexte économique global qui incite à l'économie financière et à la mutualisation des moyens, l'école a décidé de revoir sa stratégie pédagogique et de développer ses capacités dans le domaine de l'enseignement numérique. À ce titre, le projet global « Campus Area Network » (CAN) a été lancé durant l'année 2008 dans le but d'adapter l'infrastructure technique et pédagogique de l'école à sa nouvelle stratégie. L'un des piliers du projet CAN repose sur la mise en œuvre d'un portail web sécurisé nommé espace numérique de travail qui centralise l'accès à divers services numériques à vocation pédagogique, telles la consultation de documentations enrichies, le suivi de parcours de formation en ligne ou le partage de la connaissance.

Ce mémoire prend sa place au sein du projet CAN et vise à conduire une étude aboutissant à la conception et la réalisation d'une solution de diffusion des flux pédagogiques multimédias de l'espace numérique de travail. Pour cela, une analyse complète des problématiques techniques et fonctionnelles est réalisée, des choix d'architecture sont préconisés et les solutions correspondantes sont développées afin d'assurer le confort pédagogique aux stagiaires.

Mots clefs : multimédia, vidéo, architecture réseau, redondance, qualité de service.

---

## ABSTRACT

The Signal School at Cesson Sevigne is a Joint school specializing in the training of Ministry of Defense personnel in Communication Systems and Electronic Warfare. In a challenging global economic environment which demands financial savings and the rationalization of resources, the school decided to review its teaching strategy and develop a digital learning capability. To this end, the "Campus Area Network" (CAN) project was launched during 2008 with the aim of re-aligning the technical infrastructure and teaching methodology to this new approach. One of the key tenets of this new approach was the implementation of a secure web portal known as the "Digital Workspace" which provides one point of access to the various digital services, such as access to specialist documentation, training courses and knowledge sharing.

This exercise relates directly to the CAN Project and represents a study of the design and implementation of the multimedia solution delivered in the "Digital Workspace". To achieve this, a complete analysis of the technical and functional challenges has been undertaken, architectural options have been recommended and solutions developed in order to ensure that appropriate teaching support is available to students.

Key Words: Multimedia, Network Architecture, Redundancy, Quality of Service.





# Table des matières

1 : Introduction.....	7
1.1 : L'École des transmissions.....	8
1.2 : Le projet CAN/ENT.....	9
1.3 : Le projet CNAM.....	10
1.3.a)Présentation de mon projet.....	10
1.3.b)Les défis à relever.....	10
1.3.c)La démarche d'ingénierie mise en œuvre.....	11
1.3.d)Planification du projet CNAM.....	11
1.3.e)Plan du mémoire.....	12
2 : Étude de l'existant pédagogique.....	13
2.1 : État de l'art de l'enseignement numérique.....	13
2.1.a)Les différents types d'enseignement numérique.....	13
2.1.b)Analyse comparative par critères de choix.....	15
2.2 : Organisation de l'enseignement dans l'armée de Terre.....	18
2.2.a)Le modèle de fonctionnement général.....	18
2.2.b)La place de l'enseignement numérique.....	18
2.3 : Organisation de l'enseignement à l'ETRS.....	19
2.4 : Les modes de partage de la connaissance à l'ETRS.....	20
2.4.a)Le mode présentiel.....	21
2.4.b)L'enseignement à distance.....	22
2.4.c)L'indexation des ressources.....	24
2.4.d)Les cours en lignes.....	24
2.4.e)Les modes de partage de la connaissance privilégiés.....	24
2.5 : La place de l'enseignement numérique à l'ETRS.....	25
2.5.a)Organisation de l'enseignement numérique à l'ETRS.....	26
3 : Étude de l'existant technique.....	28
3.1 : Le système d'information de la formation.....	28
3.1.a)Les clients.....	29
3.1.b)Les services métier.....	29
3.1.c)La liaison entre les clients et les services métier.....	29
3.1.d)L'infrastructure du SIF.....	30
3.1.e)Les éléments reliés à infrastructure.....	30
3.2 : Le Campus Area Network.....	31
3.2.a)Le réseau d'enseignement global.....	31
3.2.b)Le réseau d'enseignement Intraterre.....	32
3.2.c)Le réseau d'enseignement Internet.....	32
3.2.d)Conséquences de l'existence de deux réseaux d'enseignement.....	33
3.3 : Les zones d'implantation géographiques du SIF.....	35
3.4 : Réduction de périmètre technique du projet CNAM.....	37
3.5 : L'espace numérique de travail.....	38
3.5.a)Présentation générale de l'espace numérique de travail.....	38
3.5.b)Présentation de l'ENT d'après les processus ITIL.....	38
3.6 : Les types de médias proposés par l'ENT.....	41
3.6.a)L'approche document.....	41
3.6.b)L'approche développeur.....	42
3.6.c)L'approche serveur.....	43
4 : Étude du besoin.....	45
4.1 : Le constat à l'origine du besoin.....	45

4.2 :L'expression du besoin.....	48
4.2.a)Les fonctionnalités souhaitées.....	48
4.2.b)Les contraintes.....	48
4.2.c)Les exigences.....	49
4.2.d)Synthèse de l'expression du besoin.....	49
5 :Conception.....	51
5.1 :Identification des services impactés par le projet.....	51
5.2 :Stratégie générale de conception.....	53
5.3 :Conception associée au service d'accès/authentification.....	56
5.3.a)Les zones élémentaires et les liaisons à prendre en compte.....	56
5.3.b)Liaison N°1 : WAN Internet et DMZ.....	56
5.3.c)Liaison n°2 : Zone hébergement et DMZ.....	60
5.3.d)Liaison n°3 : PFI/Consultation et DMZ.....	63
5.3.e)Liaison n°4 : Serveurs et DMZ.....	68
5.3.f)Liaison N°5 : Utilisateurs extérieurs/WAN Internet.....	70
5.4 :Conception associée au service de cours en ligne.....	71
5.4.a)Les zones élémentaires et les liaisons à prendre en compte.....	71
5.4.b)Conception de la solution.....	72
6 :Réalisation.....	79
6.1 :Contexte général de réalisation.....	79
6.2 :Réalisations associées au service d'accès/authentification.....	81
6.2.a)Fonction de filtrage par serveur.....	81
6.2.b)Installation du portail captif Alcasar.....	84
6.3 :Réalisations associées au service de cours en ligne.....	88
6.4 :Synthèse.....	100
7 :Conclusion.....	102
Annexe 1 : Portefeuille des services de l'ENT.....	104
Annexe 2 : ITIL version 3.....	105
Annexe 3 : Fonction de filtrage localisée.....	107
Annexe 4 : Serveur de streaming RED5.....	109
Annexe 5 : Répartiteur de charge HAProxy.....	111
Annexe 6 : Consultation en streaming.....	113
Sigles et abréviations.....	115
Index des illustrations.....	117
Index des tableaux.....	118
Bibliographie, webographie.....	119

# 1 : INTRODUCTION

Le livre blanc de la Défense est le document de référence qui définit les objectifs de défense et de sécurité à l'échelle nationale. La dernière version<sup>1</sup>, validée par le chef de l'état durant l'année 2008, spécifie notamment des objectifs de modernisation des armées et de mutualisation des moyens. A cet effet, les différentes entités du ministère de la Défense effectuent actuellement un travail global de réorganisation en profondeur et adaptent leur modèle de fonctionnement à un contexte général qui tend à diminuer et mutualiser les ressources en personnels et en moyens.

À l'ETRS, école des transmissions du ministère de la Défense spécialisée dans le domaine des systèmes d'information et de communication, la mise en application du livre blanc de la Défense a **réduit les capacités matérielles et le nombre de formateurs affectés**, sans pour autant diminuer le calendrier des actions de formation. Pour faire face à cette situation, l'école a choisi de modifier sa stratégie pédagogique et a entrepris de **développer ses capacités dans le domaine de l'enseignement numérique**. Cette décision a été officialisée au cours de l'année 2008 lors de l'initialisation du projet « Campus Area Network » (CAN) dont l'objectif est de créer une infrastructure d'enseignement qui réponde au besoin d'une démarche globale de partage de la connaissance. Dans cette optique, l'une des actions majeures du projet CAN consiste à mettre en œuvre un espace numérique de travail accessible à partir d'un portail web. Cet espace numérique donne accès à des services qui facilitent le partage de la connaissance et doit devenir, à terme, l'outil majeur de l'École de transmissions pour dispenser de l'enseignement à distance.

Mon mémoire d'ingénieur CNAM s'inscrit dans le cadre du projet CAN et **traite de l'amélioration des capacités de diffusion des flux pédagogiques multimédias** de l'espace numérique de travail sur Internet. Pour cela, je dois **concevoir et réaliser les solutions** qui ajoutent à l'infrastructure existante la **capacité à intégrer des flux audio ou vidéo dans les ressources pédagogiques** proposées. La diffusion de ces flux audio ou vidéo doit de plus être effectuée avec un **niveau de qualité de service** tel qu'il permette une **consultation à distance**.

Les actions entreprises impactent **l'architecture technique**, tant au niveau du réseau que des applications, ainsi que les **organisations fonctionnelles** en charge de la pédagogie ou de l'administration des systèmes.

Le plan général retenu s'articule autour de la description de l'environnement, du contexte et des objectifs du mémoire. Cette étape indispensable reflète la phase d'analyse que j'ai du conduire afin de bien appréhender le contexte général dans lequel évolue le projet.

Ensuite, une phase d'étude des problématiques est menée afin de présenter et identifier le besoin. Enfin, une phase de conception et de réalisation permettent le déploiement de solutions qui répondent au besoin et assurent le confort pédagogique des stagiaires.

---

<sup>1</sup> La dernière version du livre blanc sur la Défense et la sécurité nationale est disponible à l'adresse : [http://www.livreblancdefenseetsecurite.gouv.fr/information/les\\_dossiers\\_actualites\\_19/livre\\_blanc\\_sur\\_defense\\_875/index.html](http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html)

## 1.1 : L'École des transmissions

Organisme de l'armée de terre rattaché à la direction des ressources humaines de l'armée de terre (DRHAT), l'École des transmissions (ETRS) de Cesson-Sévigné est une école interarmées qui délivre des formations à plus de 3 000 stagiaires par an dans le domaine des systèmes d'information et de communication et la guerre électronique.

D'un point de vue hiérarchique, l'ETRS est subordonnée à la sous-direction de la formation et des écoles (SDFE). Pour le soutien, elle est rattachée à la base de défense de Rennes. Cette organisation prend sa place au sein d'une structure globale ascendante qui pointe à son niveau le plus haut sur le président de la république, identifié comme le chef des armées, comme le présente le schéma ci-dessous.

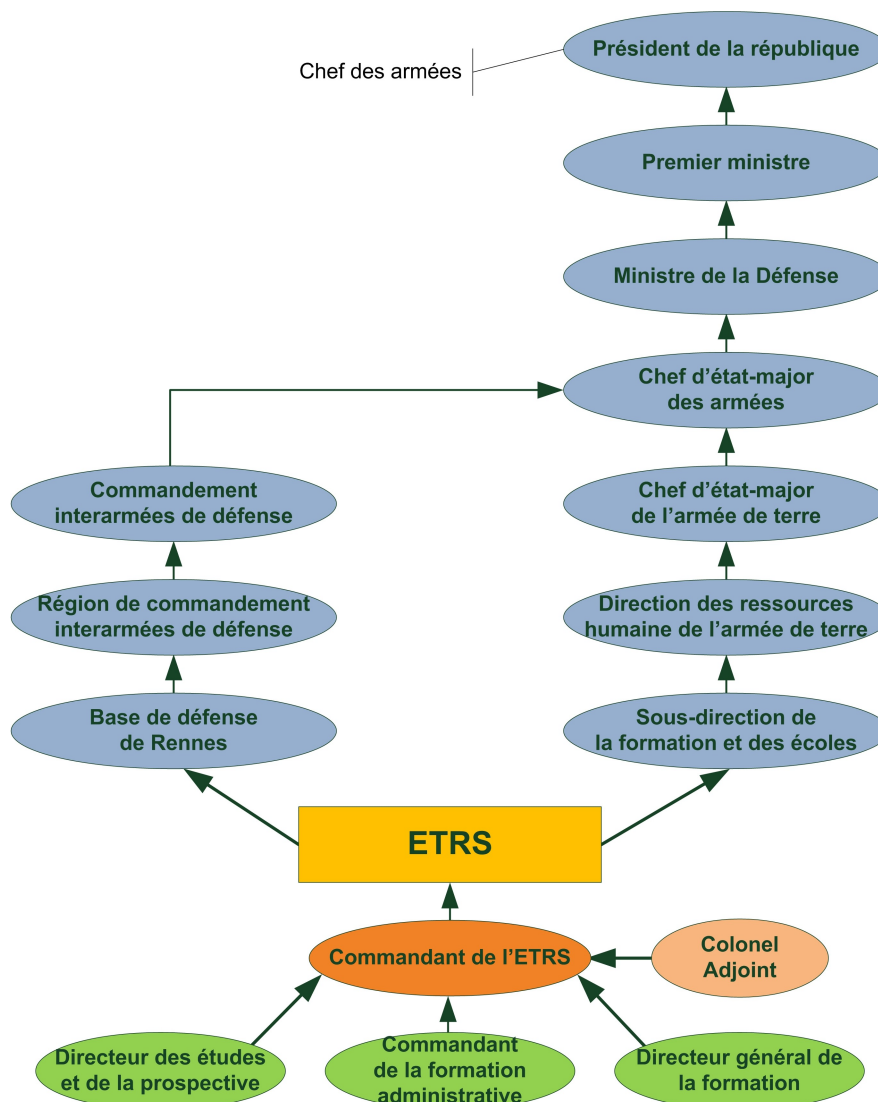


Illustration 1: Structure organisationnelle de l'ETRS

Une base de défense est à l'échelon local l'unique formation administrative de la Défense qui regroupe l'ensemble du personnel militaire et civil présent dans un secteur géographique donné, ce secteur pouvant recouvrir une ou plusieurs communes proches les unes des autres. Ce type d'organisation est de portée interarmées et a pour finalité la mutualisation des moyens, conformément à l'un des objectifs du livre blanc de la Défense.

Le rôle de la sous-direction de la formation et des écoles consiste à diriger la formation au sein de l'armée de terre et à piloter les politiques d'enseignement générales et leur mise en application. La SDFE a validé le projet de l'ETRS dans le domaine de l'enseignement numérique. Elle suit les travaux réalisés dans le cadre d'études de niveau ministériel visant à définir un schéma directeur global relatif à l'enseignement à distance.

En interne, l'école est placée sous l'autorité d'un officier général de l'armée de terre secondé par un colonel adjoint. Le colonel adjoint exerce des responsabilités transverses et a autorité pour assurer la coordination d'activités de portée globale comme la gestion de la sécurité informatique ou la gestion de la qualité.

Le directeur général de la formation participe au niveau local à la conception des actions de formation et s'assure de leur correspondance avec les directives de la SDFE.

Le directeur des études et de la prospective est responsable des recherches et prospections que mène l'école afin de définir l'emploi des systèmes dans le présent et le futur.

Enfin, le commandant de la formation administrative est responsable des activités de soutien telles que le service général, la gestion des ressources humaines ou la condition du personnel et de l'environnement humain.

## 1.2 : Le projet CAN/ENT

Le projet « Campus Area Network » (CAN) / « Espace Numérique de Travail » (ENT) a été initié en 2008 **sous la direction du colonel adjoint** dans le but d'**adapter l'infrastructure de l'ETRS à une plus grande capacité de mise en œuvre dans le domaine de l'enseignement numérique**, qu'il soit dispensé en local ou à distance. L'objectif à atteindre consiste à faire évoluer le Système d'Information de la Formation (SIF) pour lui offrir la capacité d'exploiter des services pédagogiques au format numérique. L'ingénierie relative à ce projet porte sur deux axes majeurs traitant des **aspects techniques et fonctionnels** à prendre en compte pour réussir la transformation entre l'existant et le modèle de fonctionnement futur orienté vers l'enseignement numérique. La stratégie globale du projet CAN/ENT est définie par un schéma directeur et une directive relative à l'enseignement numérique validés par le général commandant l'école.

Les travaux de l'ETRS dans le domaine de l'enseignement numérique ont conduit à déployer au sein de l'architecture technique du CAN plusieurs services permettant par exemple de suivre un parcours pédagogique en ligne, de collaborer ou de communiquer avec différents intervenants, de consulter des supports enrichis et interactifs ou de visualiser des emplois du temps. Ces services sont tous centralisés et accessibles à partir d'un portail web sécurisé nommé « Espace Numérique de Travail » (ENT) qui s'appuie sur un projet déjà en place dans de nombreuses universités et centres de recherche français. **L'espace numérique de travail est un élément majeur du projet CAN.** Le volume annuel de stagiaires qui l'utilisent pour suivre une formation est de l'ordre de 600. A terme, l'école a pour cible d'en permettre l'accès à **l'ensemble des personnels du ministère de la Défense**, depuis le territoire français ou en opération extérieure. Dans cette optique, il est donc impératif que l'infrastructure et l'architecture qui supportent l'ensemble des éléments mis en œuvre soient à même de proposer une qualité de service apte à répondre à cet objectif.

**Le projet CAN/ENT est subdivisé en plusieurs sous-projets** qui prennent chacun en charge un domaine de compétence spécifique ou une problématique donnée. Ainsi, par exemple, un sous-projet traite des moyens et prend en compte les aspects matériels, logiciels et budgétaire. Un autre gère l'aspect pédagogique et s'attache notamment aux nécessaires conversions et adaptations des

supports de cours au format numérique. Enfin, les études et les conceptions techniques, l'intégration des systèmes, la sécurisation et l'administration des services sont confiés au sous-projet en charge de l'architecture. Au sein de cette organisation, **je suis le chef du sous-projet en charge de l'architecture** et l'étude sur laquelle repose ce mémoire CNAM y est également intégrée.

Un comité de pilotage trimestriel est présidé par le général commandant l'école. En présence du colonel adjoint et des directeurs, les différents responsables de sous-projet présentent un tableau de bord des actions réalisées, l'état d'avancement de leurs travaux, exposent leurs difficultés et proposent la planification des opérations à venir.

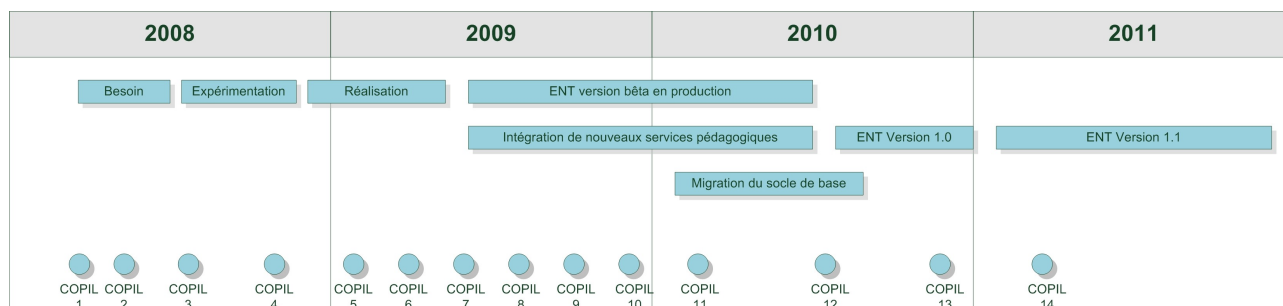


Illustration 2: Planification du projet CAN depuis son lancement

Comme le montre le planning présenté ci-dessus, les comités de pilotage accompagnent étroitement le déroulement de chaque phase du projet CAN depuis son lancement officiel durant l'année 2008.

## 1.3 : Le projet CNAM

### 1.3.a) Présentation de mon projet

Le projet CNAM qui motive ce mémoire d'ingénieur prend en compte la perspective de montée en puissance de l'espace numérique de travail et a pour objectif de s'assurer que les flux pédagogiques multimédias proposés par la plate forme sont accessibles sans temps de latence et sont fluides quels que soit l'heure et le lieu d'utilisation. Les flux multimédias sont présents en de nombreux points dans l'espace numérique de travail. Ils sont utilisés entre autres pour enrichir les supports pédagogiques avec des vidéos de cours filmés ou pour illustrer des pages web de documentation. La capacité à pouvoir accéder immédiatement à ces flux et à les consulter sans saccade est déterminante pour le succès général du projet CAN. L'expression de besoin qui motive la réalisation de ce mémoire s'appuie sur le fait que les temps d'accès et la qualité de consultation des flux multimédias actuellement proposés par l'espace numérique de travail ne remplissent pas ces conditions. En effet, suivant la localisation de l'utilisateur et les caractéristiques de la liaison mise en jeu, **les flux multimédias restitués sont dégradés voire interrompus**. Cette situation nuit au confort pédagogique des stagiaires et, par extension, à la réussite générale du projet CAN.

### 1.3.b) Les défis à relever

Les défis à relever pour ce projet sont multiples. L'architecture technique dans laquelle s'intègre l'espace numérique de travail est complexe, étendue et se subdivise en parties distinctes qui interdisent l'appréhension de l'ensemble comme un élément unique auquel il serait possible d'appliquer des solutions globales ou génériques. D'autre part, l'espace numérique de travail est déjà en production et mobilise des ressources humaines et matérielles conséquentes tant dans le domaine de l'informatique que celui de la pédagogie. Les solutions déployées ne doivent pas

provoquer d'interruption de service et doivent être pérennisées afin de rentabiliser dans le temps les coûts liés à leur conception, leur réalisation et leur mise en œuvre fonctionnelle et technique.

### 1.3.c) La démarche d'ingénierie mise en œuvre

La démarche globale d'ingénierie mise en œuvre durant la conduite de ce projet CNAM s'appuie sur le recueil de bonnes pratiques « Information Technology Infrastructure Library »<sup>2</sup> (ITIL) spécialisées dans la gestion de services informatiques. Cette approche a été imposée par M. Martineau, l'officier en management des systèmes d'information (OMSI)<sup>3</sup>, afin de s'assurer que les actions entreprises s'intègrent correctement au sein du projet CAN qui s'appuie déjà lui-même sur la démarche ITIL.

En soit, le recueil de bonnes pratiques ITIL n'est pas une méthodologie de conduite de projet. Il permet d'améliorer la qualité des systèmes d'information en proposant une approche par processus clairement définis et contrôlés lors de la définition de la stratégie, la conception, la transition ou l'exploitation des services. Un service est défini comme un ensemble d'éléments connexes fournis à l'appui d'un ou de plusieurs processus métiers. Le service est composé d'éléments de configuration mais il est perçu par les clients comme un tout. La démarche ITIL préconise de maintenir à jour un catalogue des services proposés par un système d'information afin d'identifier en permanence les processus à valeur ajoutée. Le projet CNAM impacte deux éléments identifiés au portefeuille des services de l'espace numérique de travail: le service d'accès/authentification et le service de cours en ligne<sup>4</sup>.

### 1.3.d) Planification du projet CNAM

La planification de ce projet CNAM s'inscrit au sein de deux phases majeures dédiées pour la première à l'appropriation et la consolidation du contexte général de réalisation et, pour la seconde, au déroulement effectif du projet, comme le montre le planning ci-dessous.

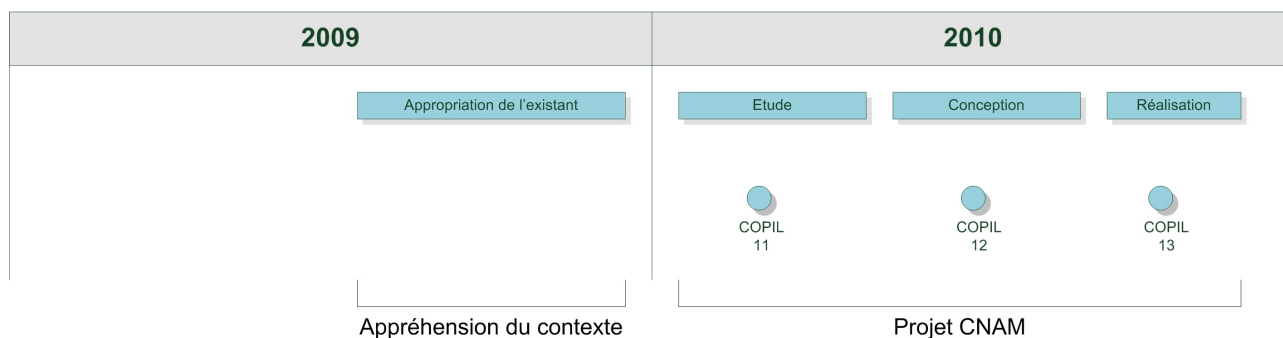


Illustration 3: Planification du projet CNAM

2 Adresse du site francophone de la démarche ITIL : <http://www.itilfrance.com>

3 La fonction OMSI au sein de la Défense est équivalente à la fonction de directeur des systèmes d'information (DSI)

4 Le portefeuille des services de l'ENT est fourni en annexe 1



### 1.3.e) Plan du mémoire

Le plan retenu pour ce mémoire débute par une étude préalable de l'existant pédagogique et de l'existant technique à laquelle s'applique une réduction de périmètre du domaine considéré. Cette étape permet de bien définir les limites de l'étude et est indispensable à la bonne compréhension générale du contexte de réalisation du projet tant au niveau fonctionnel que technique.

Soutenue par une vision globale sur l'environnement du projet, la partie qui suit présente l'étude du besoin et définit la problématique abordée en la situant au sein du système d'information de la formation.

Une partie dédiée à la conception propose alors plusieurs préconisations de solutions toutes motivées par des analyses permettant de justifier les choix réalisés.

Enfin, la dernière partie traite de la réalisation des solutions qui ont pu être développées dans le cadre de ce projet et aborde pour chacune d'entre elles les tests préalables à la mise en œuvre, les effets obtenus et un examen prospectif des perspectives d'évolution.

---

*Le projet CAN est un projet global piloté à l'École des transmissions dont l'objectif vise à mettre en œuvre un réseau d'enseignement orienté vers le partage de la connaissance et l'enseignement numérique. L'un des composants majeurs du projet est matérialisé par un espace numérique de travail de type portail web qui propose un accès centralisé à différents services contribuant à atteindre cet objectif. Le projet CAN est découpé en plusieurs sous-projets dont celui en charge de l'architecture de l'infrastructure technique mise en œuvre.*

*Le projet CNAM qui motive ce mémoire est rattaché au sous-projet « architecture » du projet CAN et a pour objectif de permettre l'intégration et la consultation de flux audio ou vidéo au sein des ressources pédagogiques proposées par l'espace numérique de travail. Actuellement, les capacités de la plate-forme technique mise en œuvre ne permettent pas d'envisager ce type d'utilisation.*

*Les actions à mener pour réaliser le projet sont multiples. Elles traitent par exemple de l'aspect technique et des nécessaires modifications à apporter à la configuration du réseau pour lui permettre de supporter des débits plus importants ou de la conception d'une architecture évolutive qui permettent de diffuser des flux multimédias. L'aspect fonctionnel est également impacté et nécessitent un travail collaboratif avec les acteurs en charge de la pédagogie afin d'intégrer dans l'existant les travaux réalisés.*

*Pour mieux distinguer l'environnement fonctionnel dans lequel s'intègre ce projet CNAM, la partie qui suit propose une étude de l'existant pédagogique.*

## 2 : ÉTUDE DE L'EXISTANT PÉDAGOGIQUE

*Une vision claire du contexte dans lequel s'inscrit l'enseignement numérique à l'ETRS est indispensable à la bonne compréhension du contexte global du projet. Pour cela, ce chapitre fournit une étude de l'existant pédagogique.*

*Le plan général de cette étude de l'existant pédagogique dans un premier temps sur un état de l'art de l'enseignement numérique afin de bien appréhender le périmètre technique et fonctionnel de la discipline.*

*Le second volet du chapitre fournit une analyse descendante de l'organisation de l'enseignement, d'abord au niveau de l'armée de Terre puis à celui de l'École des transmissions en apportant à chaque fois une attention particulière au positionnement de l'enseignement numérique dans la structuration.*

### 2.1 : État de l'art de l'enseignement numérique

*Pré-requis indispensable à la bonne compréhension globale du projet, la partie qui suit présente un état de l'art de l'enseignement numérique et permet de mieux connaître les différents concepts et techniques relatifs au domaine.*

L'enseignement numérique répond à des besoins de personnalisation, d'individualisation et de délocalisation des cursus de formation et facilite l'accès aux ressources pédagogiques employées.

#### 2.1.a) Les différents types d'enseignement numérique

Le domaine de l'enseignement numérique évolue actuellement autour de quatre axes majeurs :

- **L'enseignement assisté par ordinateur (EAO)** : Il met en œuvre un ordinateur sur lequel s'exécute un programme destiné à transmettre la connaissance
- **La simulation** : Elle est utilisée pour imiter une situation réelle ou reproduire le fonctionnement d'un système donné.
- **L'enseignement à distance (EAD)** : C'est l'évolution de l'enseignement assisté par ordinateur. Il met en jeu des technologies modernes d'information et de communication.
- **Les salles de classe simulées (classes virtuelles)** : Elles mettent en œuvre des outils qui permettent de simuler à distance l'interactivité d'une classe réelle.

#### **- L'enseignement assisté par ordinateur (EAO)**

L'enseignement assisté par ordinateur est le **pionnier historique de l'enseignement numérique**. Il apparaît au début des années 90 avec l'avènement du CDROM multimédia.

Dans une salle de cours, un bureau ou à domicile, l'apprenant<sup>5</sup> est assisté par un ordinateur et un logiciel adapté au contenu de sa formation. Ce mode d'enseignement ne nécessite pas de connexion réseau et ne met pas en jeu d'interaction avec un professeur ou d'autres élèves. De plus, la progression de l'apprenant n'est pas individualisée.

Il peut s'agir de didacticiels présentant le fonctionnement de systèmes ou de différents recueils de documentations électroniques relatives à un thème donné. Les logiciels d'EAO sont disponibles sur

---

<sup>5</sup> « **Apprenant** » est un terme générique qui désigne une personne physique exécutant un processus d'apprentissage. Il peut s'agir d'un stagiaire ou d'un individu isolé qui souhaite acquérir des connaissances.

étagère dans les grandes surfaces ou depuis les sites de ventes en ligne. Les premiers prix débutent à quelques dizaines d'euros.

### **- La simulation**

La simulation est un type d'enseignement numérique dont le but est de mettre en œuvre des situations réelles dans un environnement virtuel. Elle apparaît dans les années 80 avec l'arrivée des premiers ordinateurs proposant une puissance de calcul réellement exploitable.

Son intérêt réside dans le fait qu'elle permet de jouer des mises en situation, de s'entraîner ou de préparer et évaluer des scénarios variés.

Il existe deux types principaux de simulateurs :

- Les simulateurs métiers qui contiennent de grandes quantités de règles de gestion spécifiques à un thème donné et permettent des mises en situation cohérentes,
- Les simulateurs techniques développés pour recopier le fonctionnement de systèmes spécifiques. Ils sont généralement conçus par les industriels eux même.

L'offre en simulateurs débute à quelques dizaines d'euros pour les plus simples, tels les jeux de simulation disponibles dans le commerce et peut atteindre plusieurs millions d'euros pour les plus complexes, tels les simulateurs de vols aériens développés par les industriels de l'aéronautique.

### **- L'enseignement à distance (EAD)**

L'enseignement à distance est le **concept le plus récent de l'enseignement numérique**.

Il apparaît au début des années 2000 et permet de suivre à distance des parcours pédagogiques complets et individualisés.

Le système s'adapte au rythme d'évolution de l'apprenant, propose un suivi personnalisé et peut dérouler des processus de validation des connaissances. C'est une évolution de l'enseignement assisté par ordinateur qui met l'accent sur la qualité du lien entre l'apprenant et la ressource pédagogique en proposant une plus grande interactivité.

Grâce à une connexion réseau, le système peut être mis à jour, l'apprenant peut communiquer par mail ou forum et un formateur distant peut participer aux cursus de formation. Les services mis en œuvre en enseignement à distance sont généralement **développées avec des technologies web et s'utilisent à partir de navigateurs Internet** sans nécessiter l'installation de logiciels spécialisés.

Aujourd'hui, l'enseignement à distance permet d'obtenir des diplômes, des certifications, de valider des acquis par l'expérience. C'est un mode de formation utilisé par les universités, par le conservatoire nationale des arts et métiers (CNAM) ou encore par le centre nationale d'éducation à distance (CNED).

Le coût d'une plate-forme d'enseignement à distance est élevé et s'exprime en dizaines de milliers d'euros. Cette dépense est inhérente aux investissements matériels nécessaires à l'acquisition des serveurs et aux investissements fonctionnels liés à la mise en place d'une organisation adaptée.

## **- La salle de classe simulée (ou classe virtuelle)**

La classe virtuelle désigne la simulation d'une classe réelle. Son objectif vise à recréer à distance les interactions d'une salle de cours. Elle s'appuie sur l'animation de sessions synchrones, à une date et une heure données, entre un animateur et des apprenants.

Les outils mis en jeu reposent sur la communication en temps réel et favorisent la communication écrite ou orale grâce à la mise en œuvre de services tels que la visioconférence ou la messagerie instantanée. Ils exploitent généralement des contenus pédagogiques déjà hébergés par une plateforme d'enseignement à distance.

### **2.1.b) Analyse comparative par critères de choix**

Le tableau de synthèse de la page suivante présente une étude comparative des différents modes d'enseignement numérique en fonction de critères de choix. Les différents points abordés dans le paragraphe précédent et l'analyse du tableau de synthèse permettent de dégager les éléments suivants :

**L'enseignement assisté par ordinateur (EAO) est simple à mettre en œuvre et peu onéreux** mais son utilisation est majoritairement réservée à **un poste local isolé**. **L'interaction avec l'apprenant est faible** car l'EAO obéit à des règles strictes et répétitives qui peuvent s'apparenter au fonctionnement de **systèmes automatiques**. L'enseignement assisté par ordinateur est généralement **utilisé en soutien** mais ne se présente pas comme seul moyen de formation pour une matière ou une discipline donnée.

Dans la majeure partie des cas, **la simulation est nativement conçue pour permettre une grande interactivité avec l'utilisateur** car son mode de fonctionnement est prévu pour réagir en fonction de réactions ou de décisions. En revanche, **la simulation favorise l'acquisition de l'expérience mais ne permet qu'une faible transmission des connaissances**. En effet, soit la connaissance est acquise avant la séance et la simulation est utilisée pour effectuer une mise en pratique, soit la connaissance est obtenue à posteriori lors de l'analyse des comportements et des réactions observés durant la séance.

La salle de classe simulée, ou classe virtuelle, **permet une grande interactivité et une bonne transmission des connaissances** mais son **utilisation reste réservée à un groupe de personnes** et non à un individu isolé. De ce fait, un apprenant unique ne peut envisager d'utiliser ce type d'enseignement numérique pour suivre un parcours de formation personnalisé.

L'enseignement à distance nécessite la mise en place d'une **architecture complexe, globalement onéreuse**, qui met en œuvre de nombreux serveurs informatiques et des moyens techniques et fonctionnels importants. Il impose de **revoir en profondeur l'organisation fonctionnelle des parcours de formation**. En revanche, **l'interaction avec l'apprenant est élevée car les comportements et les contenus sont personnalisés** en fonction du parcours des individus. De plus, l'accès est immédiat et les contraintes géographiques sont levées. L'enseignement à distance est le type d'enseignement numérique qui **répond le plus au besoin de personnalisation, d'individualisation et de délocalisation des parcours de formation**. Il simplifie également l'accès aux ressources grâce à l'utilisation de technologies qui permettent de les atteindre à distance, tels les navigateurs web et les sites Internet.

*L'enseignement numérique répond à des besoins de personnalisation, d'individualisation et de délocalisation des cursus de formation. Il se décline en quatre catégories : l'enseignement assisté par ordinateur, la simulation, l'enseignement à distance et les classes virtuelles.*

*De nos jours, les progrès de l'informatique et les moyens de communication ont considérablement amélioré les outils mis en œuvre dans chacune des catégories. Cependant, pour répondre au besoin initial de l'enseignement numérique, le fait d'être connecté à l'Internet, de proposer des contenus personnalisés riches et interactifs et d'être disponible en permanence reste un avantage décisif. Dans cet esprit, l'enseignement à distance l'emporte largement, et notamment face à son prédécesseur historique : l'enseignement assisté par ordinateur.*

Critère de choix	Type d'enseignement numérique			
	EAO	EAD	Simulation	Classe virtuelle
<b>Modèle d'architecture technique</b>	Mono-poste	Client/serveur type web	Mono-poste ou plate-forme dédiée	Client/serveur type web
<b>Matériel nécessaire à la mise en œuvre</b>	Un poste client	- Un poste client, - Une architecture complète coté serveur.	- Un poste client pour les systèmes simples, - Un plate-forme dédiée pour les systèmes complexes.	- Un poste client, - Une architecture complète coté serveur.
<b>Nécessité d'une connexion réseau pour la mise en œuvre</b>	Non	Obligatoire	Optionnelle	Obligatoire
<b>Capacité à transmettre la connaissance</b>	Oui	Oui	Faible : Les bénéfices de la simulation sont obtenus après interprétation des résultats	Oui
<b>Personnalisation du comportement par rapport à l'apprenant</b>	Faible : l'EAO obéit à des processus répétitifs et faiblement personnalisés	Élevée : l'EAD est prévu pour réagir en fonction de l'apprenant	Élevée : La simulation est prévue pour réagir en fonction de l'apprenant	Nulle : La classe virtuelle interagit avec un groupe et non avec un individu isolé
<b>Possibilité de mixer entre la formation en présentiel et l'enseignement à distance</b>	Faible car l'EAO est globalement voué à la formation en présentiel.	Oui	La simulation est généralement utilisée dans le cadre de formation en présentiel.	Intérêt limité voire nul dans le cas de formation en présentiel.
<b>Possibilité de mettre à jour les contenus</b>	Faible : une mise à jour nécessite généralement un changement de version du logiciel ou l'application d'un patch.	Élevée : les contenus sont centralisés du coté des serveurs.	Faible : Une mise à jour nécessite généralement de formuler une demande d'évolution.	Élevée : les contenus sont centralisés du coté des serveurs.
<b>Besoin d'installation d'un logiciel spécifique</b>	Indispensable dans la majeure partie des cas.	Nul du coté du client.	Indispensable dans la majeure partie des cas.	Nul du coté du client.
<b>Tarifcation</b>	A partir de quelques dizaines d'euros	- Nulle pour la partie cliente, - Plusieurs milliers d'euros coté serveur.	De quelques dizaines d'euros à plusieurs centaines de milliers d'euros.	Tarifcation liée à celle de la plate-forme d'EAD sous-jacente.

Tableau 1: Comparatif par critères de choix des types d'enseignement numérique

## 2.2 : Organisation de l'enseignement dans l'armée de Terre

L'instruction relève d'un intérêt stratégique majeur pour l'armée de Terre car elle conditionne les compétences et les connaissances du personnel. A ce titre, la formation est régie par une structure officielle et une organisation dédiée présentée dans la partie ci-dessous.

### 2.2.a) Le modèle de fonctionnement général

L'enseignement dans l'armée de Terre est pris en compte au niveau de la direction des ressources humaines de l'armée de Terre (DRHAT) et plus particulièrement au sein de la sous-direction en charge de la formation et des écoles (SDFE), comme le présente l'illustration ci-dessous.

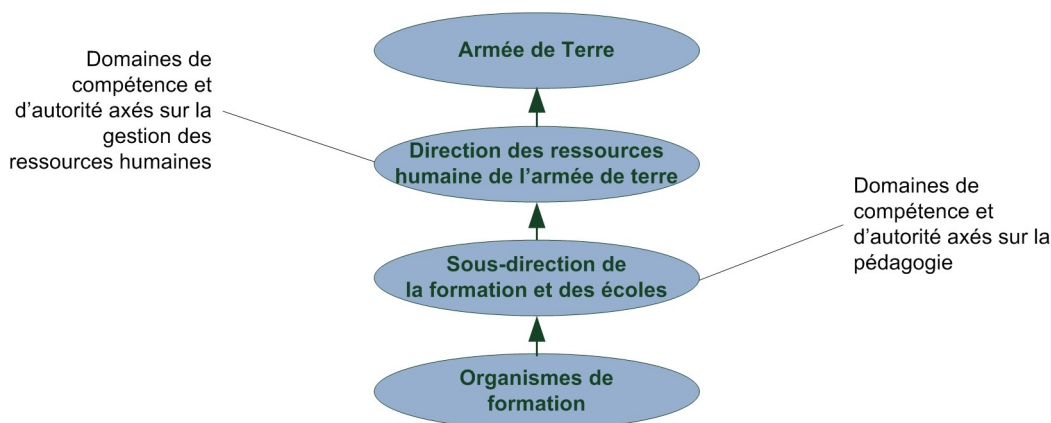


Illustration 4: Organisation de l'enseignement dans l'armée de Terre

La sous-direction en charge de la formation et des écoles est l'autorité hiérarchique directe des organismes de formation de l'armée de Terre dans le domaine de la pédagogie. Son rôle consiste à diriger la formation au sein de l'armée de Terre et à piloter les politiques d'enseignement générales ainsi que leur mise en application. Il existe plusieurs organismes de formation au sein de l'armée de Terre, tel l'École des transmissions, l'école de Saint-Cyr Coëtquidan ou l'école militaire de Paris.

La sous-direction en charge de la formation et des écoles suit avec intérêt les travaux de l'École des transmissions dans le domaine de l'enseignement numérique. Une étude est actuellement en cours pour déterminer si ce type d'enseignement doit être généralisé à l'ensemble des organismes de formation.

### 2.2.b) La place de l'enseignement numérique

Les travaux de l'École des transmissions dans le domaine de l'enseignement numérique **ne sont pas le reflet d'une initiative isolée**. D'autres organismes de formation de l'armée de Terre ont également entrepris des actions dans cette discipline. Ce constat dépasse d'ailleurs le cadre de l'armée de Terre puisque **plusieurs organismes de formation du ministère de la Défense**, comme des écoles de la marine ou de l'armée de l'air, **ont également initié des réalisations**.

Pour rationaliser et mutualiser les efforts consentis, l'enseignement numérique a été pris en compte au niveau du ministère de la Défense par le groupe de travail interarmées de l'enseignement à distance (GT IA EAD). Son mandat vise à fixer un schéma directeur de niveau ministériel permettant d'orienter l'organisation et la structuration de l'enseignement numérique. A ce jour, ce document n'est pas finalisé.

Les membres du groupes de travail appartiennent aux deux grands pôles du ministère de la Défense : la direction générale de l'armement (DGA) et les trois armées. La délégation représentative de l'armée de Terre est issue de sa structure en charge de la formation : la sous-direction de la formation et des écoles (SDFE). Enfin, quelques membres de la délégation de la SDFE appartiennent à l'ETRS.

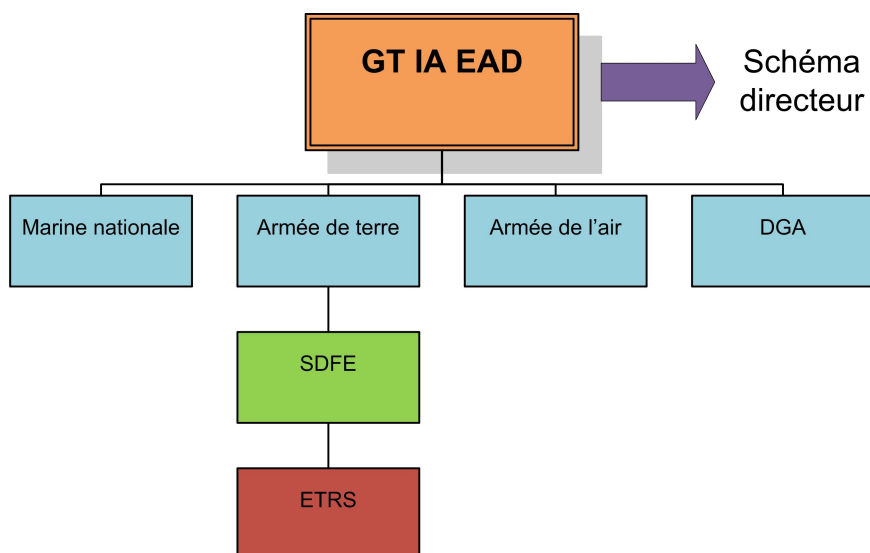


Illustration 5: Structure du GT IA EAD

Ainsi, puisque des personnels de l'ETRS participe au GT IA EAD, les travaux de l'école dans le domaine de l'enseignement numérique influent sur les éléments retenus pour élaborer le schéma directeur de niveau ministériel, comme le montre l'illustration ci-dessus.

*L'École des transmissions est rattachée à la chaîne fonctionnelle de la direction des ressources humaines de l'armée de Terre (DRHAT) et placée directement sous l'autorité de la sous-direction à la formation et des écoles (SDFE).*

*Le développement de l'enseignement numérique est pris en compte au niveau du ministère de la Défense par un groupe de travail dont l'objectif est de créer un schéma directeur de niveau ministériel. Une délégation de la SDFE appartient à ce groupe de travail et plusieurs membres de l'ETRS sont rattachés à cette délégation.*

## 2.3 : Organisation de l'enseignement à l'ETRS

**La formation est le cœur de métier de l'École des transmissions.** La partie ci-dessous présente la structure générale dans laquelle s'organise et se déroule la mission de formation de l'école. **Cette présentation est nécessaire à la bonne appréhension du contexte général dans lequel se déroule mon projet CNAM.**

La mission de formation est le cœur de métier de l'ETRS. Elle est prise en charge par la direction générale de la formation (DGF).

Le rôle de cette direction consiste à concevoir et mettre en œuvre toutes les actions de formation nécessaires à la réalisation du programme pédagogique de l'école. Pour cela, elle gère et optimise la définition, la réalisation et l'emploi des services et des ressources qui participent aux processus d'enseignement.



La structure interne de la DGF repose sur deux piliers principaux qui mettent en œuvre des divisions et des services transverses.

Les divisions représentent des pôles de compétence pédagogiques et sont spécialisées dans un domaine de formation défini. Ainsi, il existe une division pour les domaines tels que l'étude des matériels de communication militaires spécifiques, les opérations et la stratégie, l'analyse et l'exploitation des communications à des fins de renseignement ou le secteur de l'informatique générale, de la sécurité et des réseaux.

Les services transverses traitent de processus métiers nécessaires au bon fonctionnement général de la formation. Ils traitent par exemple des processus administratifs nécessaires à la gestion des flux de stagiaires ou à la mise à disposition d'ouvrages de référence à la bibliothèque.

Un système documentaire de la formation est également pris en charge par le centre de ressources SIC de l'armée de Terre (CRSICAT) installé dans les locaux de l'école. Son objectif vise à mettre en place une structure qui permette de devenir la référence la plus complète regroupant la documentation SIC au niveau de l'armée de Terre.

Les services transverses de la DGF qui mettent en œuvre des processus informatisables sont en cours d'intégration au sein de l'espace numérique de travail. Ainsi, par exemple, une application permettant d'accéder au catalogue de la bibliothèque de l'école est déjà à disposition des stagiaires.

*L'enseignement à l'ETRS est pris en compte au niveau de la direction générale de la formation qui se structure selon deux axes majeurs : des divisions prennent en charge les formations par thématique et des services transverses mettent en œuvre des processus d'assistance et de soutien.*

*La majeure partie des services transverses de la DGF qui mettent en œuvre des processus métiers informatisables feront, à terme, l'objet d'une intégration au sein de l'espace numérique de travail.*

## **2.4 : Les modes de partage de la connaissance à l'ETRS**

*La formation permet le partage de la connaissance, c'est à dire la transmission du savoir entre individus. La partie ci-dessous présente les différents mode de partage de la connaissance mis en œuvre à l'ETRS.*

Le partage de la connaissance désigne le processus de transmission du savoir entre individus et un mode de partage de la connaissance représente une méthode utilisée pour transmettre ce savoir.

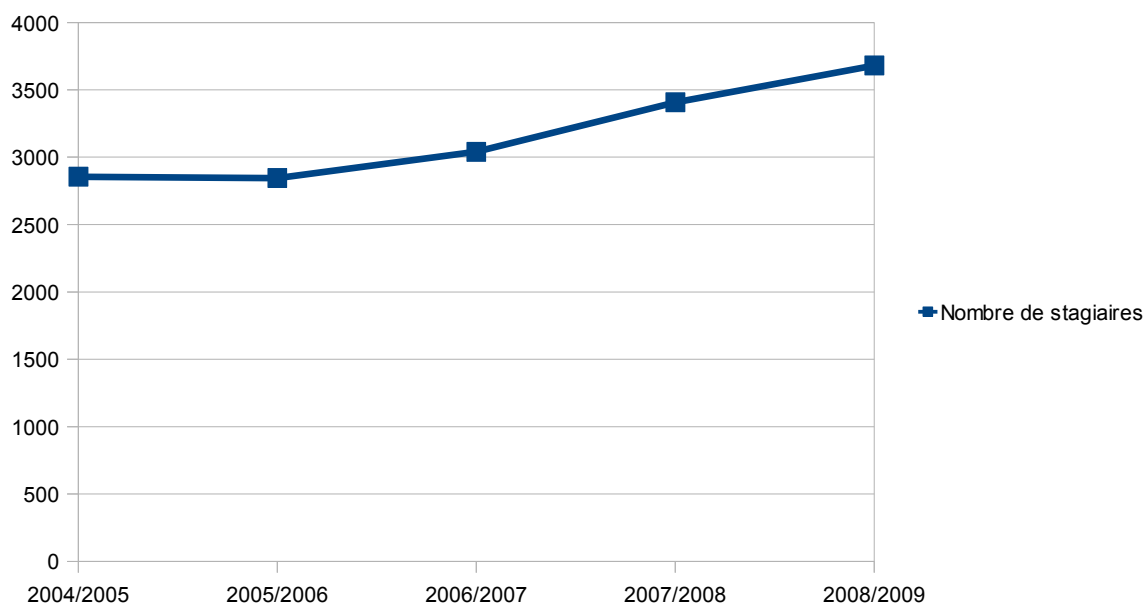
L'ETRS permet le partage de la connaissance selon quatre modes majeurs :

- Le mode présentiel : C'est le face à face pédagogique classique entre un formateur et des élèves réunis dans une salle de cours,
- L'enseignement à distance : C'est un type d'enseignement numérique qui privilégie l'interactivité et la personnalisation des parcours de formation,
- Les cours en ligne : Ce mode désigne la mise à disposition des supports de cours de l'école au format numérique,
- L'indexation des ressources : Elle favorise le partage de la connaissance en permettant un accès indexé et donc rapide aux documentations et ressources pédagogiques.

## 2.4.a) Le mode présentiel

Le mode présentiel est le mode historique de partage de la connaissance. C'est le face à face pédagogique.

Un formateur et un groupe de stagiaires sont réunis dans une salle de cours et suivent ensemble un parcours pédagogique défini. Ce parcours peut inclure des séances de cours, des travaux pratiques et/ou dirigés. Généralement, un contrôle final des connaissances valide l'acquisition du contenu pédagogique.



*Illustration 6: Évolution du nombre de stagiaires en mode présentiel par année scolaire*

**Le nombre de formations en mode présentiel est croissant depuis plusieurs années**, comme le montre l'illustration ci-dessus qui présente la progression du nombre de stagiaires mesurée par année scolaire. La raison principale de cette augmentation est liée au fait que les carrières sont plus courtes que par le passé et que la fréquence de renouvellement du personnel est plus élevée. Un rythme de recrutement plus soutenu impose un accroissement du volume de formations initiales à dispenser. D'autre part, les systèmes d'information évoluent en permanence et nécessitent des stages d'adaptation courts mais de plus en plus nombreux.

**L'évolution du nombre de stagiaires en mode présentiel s'accorde mal avec la diminution en personnel et en moyen** engendrée par la mise en application du nouveau livre blanc de la Défense. Le partage de la connaissance basé sur le mode présentiel évolue à l'école dans un contexte qui n'est pas dimensionné pour supporter la dynamique actuelle d'augmentation des volumes de formation.

## **2.4.b) L'enseignement à distance**

**L'enseignement à distance est l'alternative la plus crédible vis à vis du mode présentiel.** Il permet d'envisager une bonne adaptation à la baisse des effectifs car malgré un nombre de personnels permanents décroissant, le volume de stagiaires formés peut être beaucoup plus important.

Les premiers retours d'expérience sur le plan national de ce type d'enseignement démontrent que le niveau de qualité de formation est égal à celui du mode présentiel.

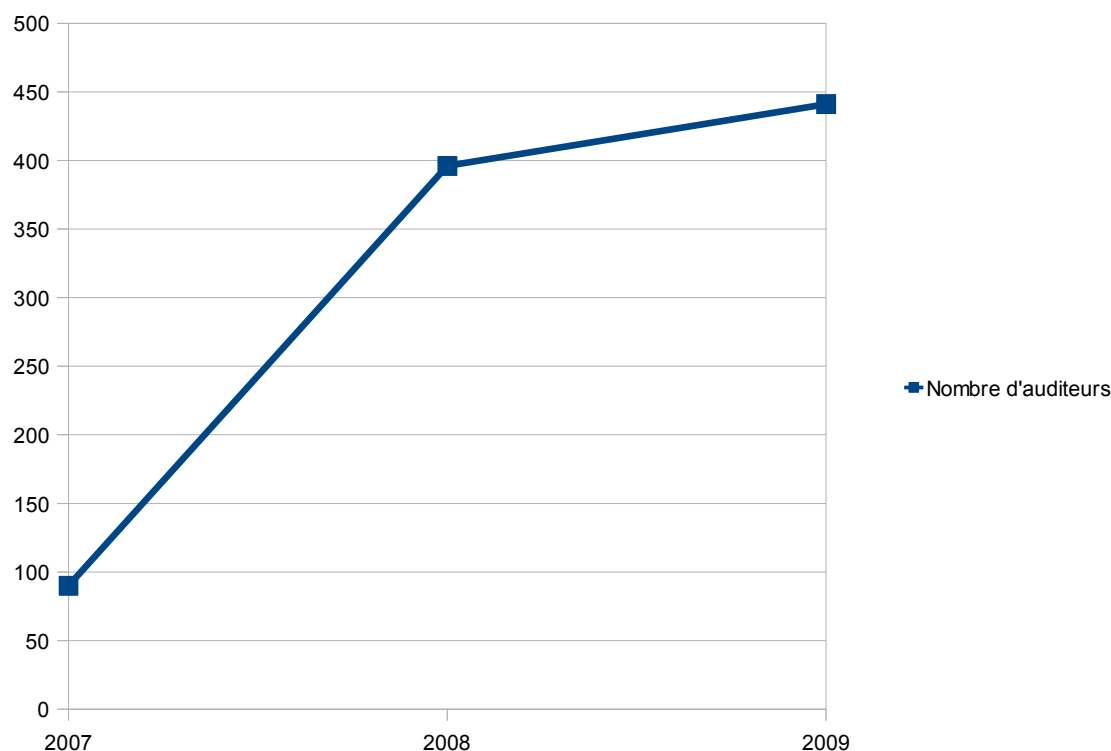
Ce mode de partage de la connaissance est encore en phase d'expérimentation au sein de l'école mais sa montée en puissance correspond à l'un des objectifs majeurs du projet CAN/ENT et a été clairement planifiée au sein du plan d'action du général actuellement en situation de commandement.

Deux modules d'enseignement à distance sont en production à l'ETRS.

### **- Le module MSIR**

Le module « systèmes informatiques et réseau » (MSIR) est un module d'enseignement à distance qui regroupe des contenus de formation communs à plusieurs stages en mode présentiel traitant d'informatique et de réseau. Les élèves inscrits à ces différents stages suivent au préalable ce module et la formation correspondante n'est plus dispensée à l'école. L'économie totale réalisée correspond ainsi à 33 heures de cours en mode présentiel. L'évaluation chiffrée financière des gains réalisés n'est pas connue.

La création de ce module a été sous-traitée et a fait l'objet d'un accompagnement pédagogique par le centre informatique de ressources multimédias (CIRM). La plate-forme met en œuvre la technologie flash et des vidéos interactives.



*Illustration 7: Évolution du nombre d'auditeurs abonnés au module MSIR par année*

Comme le présente l'illustration n°7 ci-dessus, le volume d'auditeurs inscrits au module MSIR est croissant depuis sa mise en production durant l'année 2007. Le module profite d'une bonne adoption par les stagiaires et connaît un retour d'expérience positif sur le plan pédagogique.

Le succès du module MSIR a été un facteur déterminant pour l'ETRS lors de ses réflexions sur l'adoption ou non d'une stratégie visant à développer ses capacités dans le domaine de l'enseignement numérique.

### **- Les modules CISCO**

Les modules CISCO sont quatre modules d'enseignement à distance dans le domaine des réseaux disponibles grâce à un partenariat avec la CISCO Academy<sup>6</sup>. Ils sont intéressants pour l'armée de Terre car celle-ci met en œuvre de nombreux matériels du fabricant.

Les modules sont utilisés en mode présentiel et en enseignement à distance :

- En mode présentiel, les quatre modules sont suivis durant une année par 2 classes de 20 stagiaires. Le volume correspondant en heure de cours est égal à 300.
- En enseignement à distance, le nombre d'inscription annuel moyen est de l'ordre de 130 participants.

Quel que soit le mode retenu, la validation finale des modules n'est officialisée qu'après la réussite d'une épreuve écrite à passer dans un centre CISCO.

<sup>6</sup> La CISCO Academy est l'organisme en charge des formations et des certifications de l'entreprise CISCO.

## 2.4.c) L'indexation des ressources

La centralisation, l'indexation et la mise à disposition de ressources numériques contribuent également au partage de la connaissance.

Le service repose sur la mise en ligne d'une application web basée sur le projet ORI-OAI.

ORI-OAI est un projet universitaire français développé sous licence GPL (General Public Licence). Il a pour objectif de gérer les documents numériques produits par les établissements universitaires, de les partager avec d'autres établissements, de les valoriser par une indexation professionnelle et de les rendre accessibles à distance.

Les applications compatibles avec ce modèle sont capables de s'échanger entre elles des références vers des ressources numériques pédagogiques, scientifiques et documentaires grâce à un système dit de «moissonnage d'information». Ainsi, par exemple, un site A peut récupérer toutes les nuits des références vers des ressources hébergées sur un site B et proposer dès le matin à tous ses utilisateurs l'accès à l'ensemble des ressources proposées par les sites A et B.

En France, les universités dotées d'un espace numérique de travail (ENT) participent à ce projet et partagent déjà leurs ressources. Le volume de données observé durant le moissonnage est faible car les informations échangées sont structurées en méta-données et ne véhiculent pas de contenu.

## 2.4.d) Les cours en lignes

Les cours en ligne reflètent la conversion au format numérique des supports de cours utilisés en mode présentiel. La transformation met en œuvre des documents, des vidéos, des images ou des diaporamas. A l'heure actuelle, le volume de cours dispensés à l'ETRS n'a pas encore été totalement transformé mais l'on dénombre déjà environ 300 vidéos de cours filmés et plusieurs centaines de documents numériques.

La faible interactivité et l'impossibilité de personnaliser les cours en ligne en fonction de chaque stagiaire ne permettent pas de classer ce mode de partage de la connaissance comme une déclinaison de l'enseignement à distance. C'est pour cela qu'un projet de mise en œuvre de système de gestion de l'apprentissage (« Learning Management System », LMS) est actuellement en cours de réalisation à l'ETRS. Ces systèmes mettent en œuvre des technologies de communication et d'information modernes qui permettent d'ajouter l'interactivité et la capacité d'individualisation propres à l'enseignement à distance. A terme, la totalité des cours en lignes doit être intégrée au système LMS afin de proposer les parcours de formation correspondants en enseignement à distance.

## 2.4.e) Les modes de partage de la connaissance privilégiés

A l'instar de nombreuses écoles, **l'ETRS a d'abord fondé son organisation sur le partage de la connaissance en mode présentiel** avec des salles de cours, des formateurs et des stagiaires présents sur site. Aujourd'hui, avec les restructurations et les réformes budgétaires en cours, ce mode de partage de la connaissance ne peut plus être aussi dominant car il existe une incompatibilité entre le volume de stagiaires à former et les capacités internes de l'école à mettre en œuvre le mode présentiel.

Plutôt que réduire le volume annuel de formations à dispenser, **la stratégie de l'école consiste à migrer vers un enseignement de type mixte**. Les pré-requis indispensables au suivi d'un stage

seraient dispensés en enseignement à distance tandis que le contenu principal de la formation serait enseigné en mode présentiel. Enfin, la possibilité d'entretenir a posteriori les acquis reçus durant la phase en mode présentiel serait facilitée par des modules en enseignement à distance.

Cette organisation de type mixte entre le mode de partage de la connaissance présentiel et à distance permettra de faire face au nouveau format humain et matériel de l'école sans nuire à la qualité et au volume des formations proposées. C'est dans cette perspective qu'a été initié le projet CAN durant l'année 2008 et l'espace numérique de travail représente l'interface incontournable de cette nouvelle orientation. La montée en puissance de **l'enseignement à distance relève donc d'un intérêt majeur** pour l'École des transmissions car sa capacité à **honorer le volume annuel de formation à dispenser est étroitement lié à ses capacités à opérer selon ce mode de partage de la connaissance.**

*Le rôle de l'École des transmissions est de partager la connaissance, c'est à dire de dispenser et entretenir le savoir entre individus. L'ETRS sait dispenser le savoir selon quatre modes majeur : le mode présentiel en salle de cours, l'enseignement à distance qui permet un apprentissage délocalisé interactif et individualisé, les cours en ligne et l'indexation des ressources.*

*Face à l'augmentation du nombre de formations à dispenser et la diminution des moyens en personnel et en matériel, l'École des transmissions privilégie aujourd'hui une formule mixte de partage de la connaissance basée sur le mode présentiel et l'enseignement à distance.*

## **2.5 : La place de l'enseignement numérique à l'ETRS**

*L'enseignement à distance est un type d'enseignement numérique totalement intégré à la stratégie de partage de la connaissance de l'École des transmissions mais l'ETRS met également en œuvre d'autres types d'enseignement numérique.*

*La partie qui suit expose une analyse de l'utilisation des différents types d'enseignement numérique au sein des modes de partage de la connaissance de l'école.*

Il existe des relations croisées entre les différents modes de partage de la connaissance mis en œuvre à l'ETRS et les différents types d'enseignement numérique recensés dans l'état de l'art du début de ce chapitre. En d'autres termes, les modes de partage de la connaissance peuvent mettre en œuvre un ou plusieurs type d'enseignement numérique

### **- L'enseignement assisté par ordinateur**

L'ETRS met en œuvre l'enseignement assisté par ordinateur depuis une vingtaine d'année au sein du mode de partage de la connaissance présentiel. On recense son utilisation au travers de quelques cours traitant de systèmes métiers spécifiques mais aussi, et surtout, au sein des laboratoires de langues utilisés pour former les personnels aux langues vivantes et au vocabulaire spécifique du domaine militaire.

La stratégie de développement de l'enseignement assisté par ordinateur retenue à l'ETRS prévoit un maintien dans le temps de l'existant sans pour autant favoriser un essor de cette discipline.

### **- L'enseignement à distance**

L'enseignement à distance est un type d'enseignement numérique qui représente à lui seul un mode de partage de la connaissance identifié à l'ETRS.

Son utilisation naturelle sous-entend une délocalisation de l'apprenant mais ce type d'enseignement numérique est également exploité au sein du mode de partage de la connaissance présentiel lors de la mise en œuvre des modules CISCO. Cette organisation apporte un double bénéfice pour l'ETRS car elle peut ainsi intégrer des fonctionnalités d'enseignement numérique dans les cours qu'elle dispense en présentiel tout en mettant en œuvre à partir des mêmes équipements une politique d'enseignement à distance.

A terme, l'intégration programmée des supports de cours dans une plate-forme de gestion de l'apprentissage (Learning Management System, LMS) permettra de mutualiser les ressources pédagogiques utilisées au sein des modes de partage de la connaissance en présentiel et en enseignement à distance.

### **- La simulation**

La simulation est utilisée à l'ETRS au sein du mode de partage de la connaissance présentiel pour former les stagiaires sur des points particuliers d'utilisation de systèmes techniques et sur la conduite des opérations. Par exemple, les apprenants utilisent des systèmes de simulation pour s'entraîner à déployer les architectures réseau spécifiques à quelques plates-formes techniques militaires.

L'ETRS souhaite renforcer ses capacités dans le domaine de la simulation et a choisi une stratégie qui vise à en favoriser le développement et l'intégration au sein de ses parcours de formation en mode présentiel.

### **- La salle de classe virtuelle**

La salle de classe virtuelle n'est pas mise en œuvre au sein de l'ETRS. Compte tenu de la nécessité de disposer d'une plate-forme d'enseignement à distance valide et opérationnelle pour mettre en œuvre ce type d'enseignement numérique, la stratégie retenue consiste pour le moment à valider les capacités opérationnelles de l'espace numérique de travail dans son environnement de production avant de s'orienter vers les classes virtuelles.

## **2.5.a) Organisation de l'enseignement numérique à l'ETRS**

La coordination et la mise en œuvre de l'enseignement numérique à l'École des transmissions sont assurées par le bureau d'enseignement numérique et simulation (BENS). Ce bureau est l'équivalent des cellules TICE (technologies de l'information et de communication pour l'éducation) des organismes de l'éducation nationale. Le BENS traite principalement d'ingénierie pédagogique et s'attache à concevoir et mettre en œuvre des solutions qui permettent d'adapter le système d'information de la formation au domaine de l'enseignement numérique. Les actions entreprises concernent par exemple la conversion des supports de cours au format numérique, la modification des programmes de formation ou l'utilisation d'outils spécialisés et dédiés aux formateurs.

La mise en œuvre de l'enseignement numérique nécessite de disposer d'un socle informatisé. Le système d'information informatisé de la formation est géré par le bureau de formation assistée par ordinateur (BFAO). Cette entité correspond à la direction des systèmes d'information (DSI) des entreprises privées. Au sein de ce bureau, une cellule architecture constituée de cinq personnes est responsable de la cohérence et de l'adaptation des plates-formes techniques vis à vis des objectifs fonctionnels à assurer. Ma position au sein de cette organisation consiste à être le responsable de la cellule architecture et c'est depuis cette cellule que le projet CNAM qui motive ce mémoire a été

réalisé.

*Les différents modes de partage de la connaissance de l'ETRS exploitent trois types d'enseignement numérique : l'enseignement assisté par ordinateur, la simulation et l'enseignement à distance, ce dernier étant le plus représenté.*

*Deux entités identifiées dans l'organisation de l'école participe à cette action :*

- *Le bureau enseignement numérique et simulation (BENS) traite de l'ingénierie pédagogique nécessaire à la couverture des aspects fonctionnels tels que la conversion des supports de cours au format numérique ou l'adaptation des processus métiers.*
- *Le bureau de formation assisté par ordinateur (BFAO) gère pour sa part les systèmes techniques informatiques associés aux plates-formes d'enseignement numérique. C'est depuis ce bureau, au sein de la cellule architecture, que le projet CNAM sur lequel repose ce mémoire a été traité.*

---

*Ce chapitre met en avant le fait que l'ETRS traverse actuellement **une période de mutation qui l'amène à revoir en profondeur son modèle de fonctionnement global et pédagogique.** Cette transformation est liée à de nouvelles contraintes organisationnelles et budgétaires ainsi qu'à des ambitions opérationnelles visant à délocaliser les processus de formation pour économiser les ressources locales.*

*Pour mener cette évolution, l'École des transmissions **procède actuellement à l'intégration de l'enseignement numérique dans son modèle pédagogique.** Cette adaptation offre de nouveaux outils et de nouvelles méthodes pour diffuser le savoir et partager la connaissance.*

*Historiquement, le mode de partage de la connaissance privilégié de l'ETRS reposait sur une organisation en présentiel mêlant formateurs et stagiaires réunis dans une salle de cours. L'intégration de l'enseignement numérique dans les processus de formation permet aujourd'hui à l'ETRS de partager la connaissance en enseignement à distance.*

*Cette caractéristique relève d'un intérêt stratégique majeur pour l'école car celle-ci doit faire face à une augmentation des formations à assurer malgré une diminution conjointe de ses moyens.*



### 3 : ÉTUDE DE L'EXISTANT TECHNIQUE

Dans la continuité du chapitre précédent, l'étude de l'existant technique est un complément indispensable à la compréhension de l'environnement dans lequel évolue mon projet CNAM.

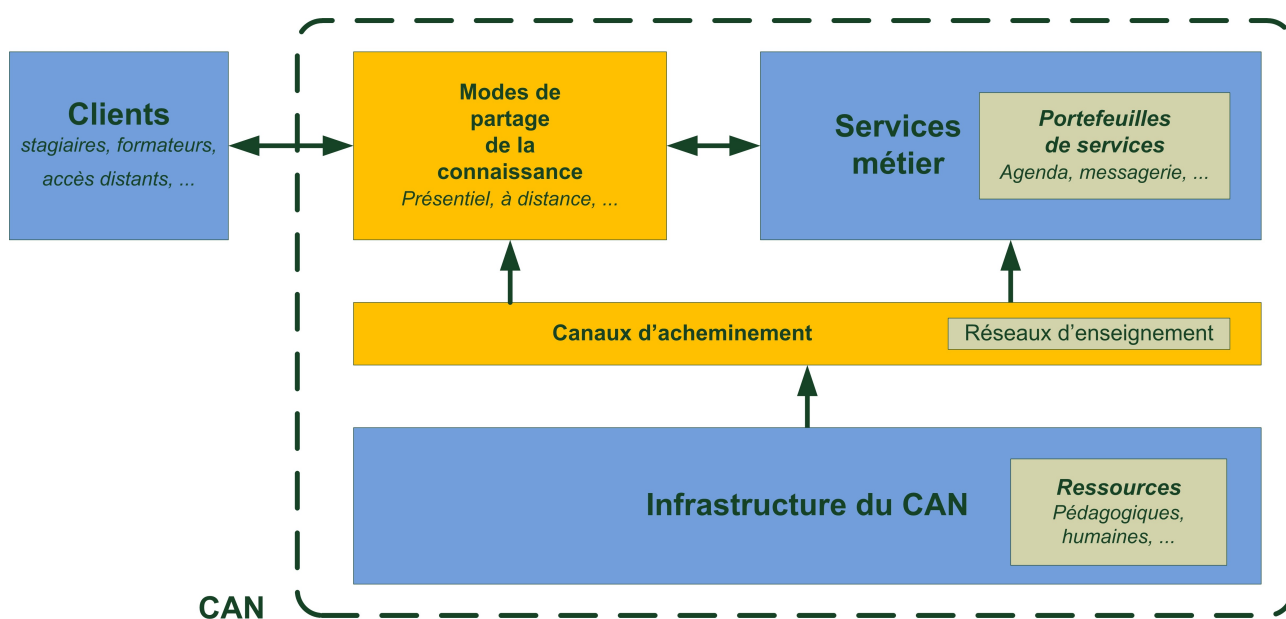
Pour cela, le chapitre présente dans un premier temps le système d'information de la formation et étudie ensuite les différents éléments techniques qui participent à sa mise en œuvre. A chaque fois, l'accent est porté sur les aspects qui concernent le projet CAN/ENT.

#### 3.1 : Le système d'information de la formation

Pré-requis indispensable à la suite de ce chapitre, cette partie définit le système d'information de la formation de l'école et présente son modèle de fonctionnement.

Le système d'information de la formation (SIF) est mis en œuvre au sein de l'École des transmissions pour assurer l'exécution des processus métiers relatifs à l'enseignement.

Comme le montre l'illustration ci-dessous, le modèle de fonctionnement du SIF repose sur trois composant principaux : des clients, des services métier et une infrastructure.



Légende :

Composant principal

Élément de liaison

Élément constitutif

Illustration 8: Modèle de fonctionnement du système d'information de la formation

La méthode de lecture du modèle s'effectue de gauche à droite, en partant des clients pour finir aux services métier reliés entre eux par les modes de partage de la connaissance. Le composant infrastructure est un composant transverse qui fournit des ressources au modèle.

Les paragraphes qui suivent proposent une étude détaillée des éléments du modèle et des relations qui les unissent.

### 3.1.a) Les clients

Les clients représentent les bénéficiaires du système d'information. Il s'agit des apprenants qui consomment les services proposés par le SIF. Ils reçoivent en échange une valeur ajoutée matérialisée par l'acquisition et l'entretien de connaissances.

**La vocation interarmées** de l'École des transmissions élargit le potentiel de client du SIF à **tout le personnel du ministère de la Défense**. La mise en œuvre de l'enseignement à distance permettra d'envisager, à terme, la délocalisation partielle ou totale des cursus de formation.

### 3.1.b) Les services métier

L'exécution des services métier permettent la production et la transmission des connaissances. Ils représentent une fonction ou une fonctionnalité identifiée et définie. Un service est une entité autonome. Il est divisé en opérations qui constituent autant d'actions spécifiques que le service peut réaliser.

La capacité à organiser une séance de formation, à gérer les emplois du temps ou à fournir des documentations sont des exemples de services proposés par le SIF. L'espace numérique de travail est un constituant du SIF. A ce titre, l'ensemble de ses services identifiés au portefeuille de services<sup>7</sup>, tels les listes de diffusion, la messagerie, les forums communautaires ou les cours en lignes viennent compléter l'offre globale de services métier proposés par le SIF.

Pour fonctionner, les services métier utilisent quatre types de ressources :

- Des ressources **pédagogiques**, tels les supports de cours ou les documentations,
- Des ressources **matérielles**, telles les plates-formes techniques mise en œuvre dans les cours de formation aux réseaux informatiques ou à l'exploitation des matériels de transmission,
- Des ressources **informatiques** fournies par des serveurs ou des programmes spécifiques, tels des services d'annuaire, des base de données, des logiciels,
- Des ressources **humaines** nécessaires à la mise en œuvre tant sur le plan technique que fonctionnel, tels les informaticiens ou les formateurs.

### 3.1.c) La liaison entre les clients et les services métier

Les clients accèdent aux services métier au travers des différents modes de partage de la connaissance recensés dans l'étude de l'existant pédagogique : le mode présentiel, l'enseignement à distance, les cours en ligne et l'indexation des ressources.

La liaison est bidirectionnelle car les interactions sont possibles dans les deux sens. Par exemple, les clients peuvent solliciter les services métiers en leur fournissant des paramètres et ces derniers leur renvoient en échange une réponse personnalisée ou une sélection de données.

La liaison entre les clients et les services métier est localisée dans le cas du mode de partage de la connaissance en présentiel et délocalisée pour l'enseignement à distance, les cours en ligne et l'indexation des ressources. L'accès aux ressources indexées est délocalisé grâce à un service disponible dans l'espace numérique de travail qui permet la consultation des informations à distance.

Les différents modes de partage de la connaissance consomment eux aussi des ressources pédagogiques, matérielles, informatiques et humaines pour réaliser les échanges entre les clients et

---

<sup>7</sup> Le portefeuille de services de l'espace numérique de travail est fourni en annexe 1

les services métier.

### 3.1.d) L'infrastructure du SIF

L'infrastructure désigne le socle sur lequel repose le système d'information de la formation. Son rôle consiste à **générer et fournir aux services métier et aux modes de partage de la connaissance les ressources nécessaires à leur fonctionnement**. Comme cela a déjà été présenté, ces ressources peuvent être de type pédagogique, matérielle, informatique ou humaine.

Par exemple, les ressources pédagogiques sont réalisées par les formateurs et sont capitalisées grâce à la rédaction de supports de cours ou de documents. Les ressources matérielles sont disponibles grâce à l'achat et la gestion des équipements. Les ressources informatiques sont fournies par des architectures informatisées dédiées à la pédagogie. Enfin, tout le personnel de l'école participe directement ou indirectement à la servitude des ressources humaines.

### 3.1.e) Les éléments reliés à infrastructure

L'infrastructure transmet ses ressources aux services métier et aux modes de partage de la connaissance grâce à des canaux d'acheminement.

La nature parfois subjective des canaux d'acheminement peut rendre difficile leur identification ou leur matérialisation. Par exemple, le véritable canal emprunté par une ressource pédagogique tel qu'un support de cours, depuis sa création jusqu'à son exploitation, est difficile à discerner tant ce type de document a parfois été modifié durant plusieurs années par des formateurs différents.

En revanche, parmi tous les canaux mis en œuvre, il en existe un qui est clairement identifié et maîtrisé au sein de l'organisation. Il s'agit du **lien exploité par les ressources informatiques**. Ces ressources sont générées par des serveurs et sont acheminées grâce à des éléments actifs (hub, switch, commutateur) et des liaisons dédiées qui forment **le réseau d'enseignement**. A titre d'illustration, c'est le réseau d'enseignement qui est utilisé lorsqu'il s'agit de transmettre une ressource pédagogique numérisée jusqu'au navigateur d'un client. A un niveau plus global, l'ensemble de l'espace numérique de travail est dépendant du réseau d'enseignement pour fonctionner et mettre en œuvre ses flux de circulation d'information.

Pour le moment, la majeure partie des équipements du réseau d'enseignement sont utilisés conjointement à ceux du réseau bureautique. Cependant, dans son mode de gestion, le réseau d'enseignement est **une entité logique** traité de manière autonome et indépendante du réseau bureautique. L'objectif, à terme, étant d'être capable de dissocier physiquement les deux.

Le réseau d'enseignement de l'école est l'un des vecteurs d'acheminement de ressource informatiques indispensable et stratégique au sein du système d'information de la formation. Il sera analysé plus en détail dans la suite de ce chapitre car il constitue à lui seul un centre d'intérêt majeur. Le projet CAN a d'ailleurs pour objectif général la rationalisation et l'amélioration du réseau d'enseignement.

L'objectif de ce projet CNAM vise quant à lui à **optimiser les ressources et les canaux d'acheminement qui participent à la circulation des flux multimédias pédagogiques de l'école**. A ce titre, le réseau d'enseignement est fortement impacté. Cet aspect sera développé plus en détail dans l'étude du besoin.

*Le modèle de fonctionnement du système d'information de la formation (SIF) met en œuvre trois*

*composants principaux : des clients, des services métier et une infrastructure.*

*Les services métier permettent de transmettre et partager la connaissance. Ils interagissent avec les clients au travers des différents mode de partage de la connaissance.*

*Pour fonctionner, les modes de partage de la connaissance et les services métier consomment des ressources pédagogiques, matérielles, informatiques et humaines. Ces ressources sont fournies par l'infrastructure et transitent entre les éléments au travers de canaux d'acheminement.*

*Le réseau d'enseignement est le canal d'acheminement qui permet le transport des ressources informatiques. Le réseau d'enseignement est d'une importance majeure pour l'école et justifie à lui seul l'existence du projet CAN dont l'objectif est de le rationaliser et l'améliorer.*

*Enfin, ce projet CNAM traite pour sa part de l'amélioration des ressources et des canaux d'acheminement qui participent à la mise en œuvre des flux pédagogiques multimédias du SIF.*

## **3.2 : Le Campus Area Network**

*Dans la partie précédente, nous avons vu que les services métier informatisés du système d'information de la formation sont approvisionnés en ressources informatiques par une connexion au réseau d'enseignement.*

*Dans les faits, il existe plusieurs réseaux d'enseignement physiques à l'école qui forment le réseau d'enseignement global. La partie qui suit présente donc une description du Campus Area Network, de son réseau d'enseignement global et des réseaux d'enseignement physiques qui le composent.*

### **3.2.a) Le réseau d'enseignement global**

Le Campus Area Network (CAN) désigne l'infrastructure globale sur laquelle s'appuient le réseau d'enseignement utilisé pour transmettre les ressources informatiques aux services métier et aux modes de partage de la connaissance. Cette infrastructure participe au modèle de fonctionnement du système d'information de la formation représentée par l'illustration n°8.

Le CAN prend naissance en 2008 lors du projet de refonte et d'adaptation de l'infrastructure de formation à la nouvelle stratégie de l'ETRS qui souhaite alors développer ses capacités d'enseignement à distance. Cette infrastructure intègre **deux réseaux informatiques physiques** : le réseau **Internet** et un réseau intranet de l'armée de Terre nommé « **Intraterre** ».

L'existence de deux réseaux se justifie par le fait que selon la politique de sécurité informatique de l'armée de Terre (PSIAT)<sup>8</sup>, les données protégées par un caractère de confidentialité ne doivent pas circuler sur le réseau Internet. De ce fait, les ressources pédagogiques qui traitent d'un domaine d'information classifié « diffusion restreinte » ou « confidentiel défense », tel le fonctionnement d'un système de transmission radio ou de guerre électronique, ne doivent pas circuler librement sur le réseau Internet. Cette distinction entre le réseau d'enseignement global et les deux réseaux d'enseignement physiques qui le composent est représentée par l'illustration ci-dessous.

---

8 La PSIAT est accessible via la note n° 1727/DEF/EMAT/BSIC/SSIC/DR/71 du 31/10/2001

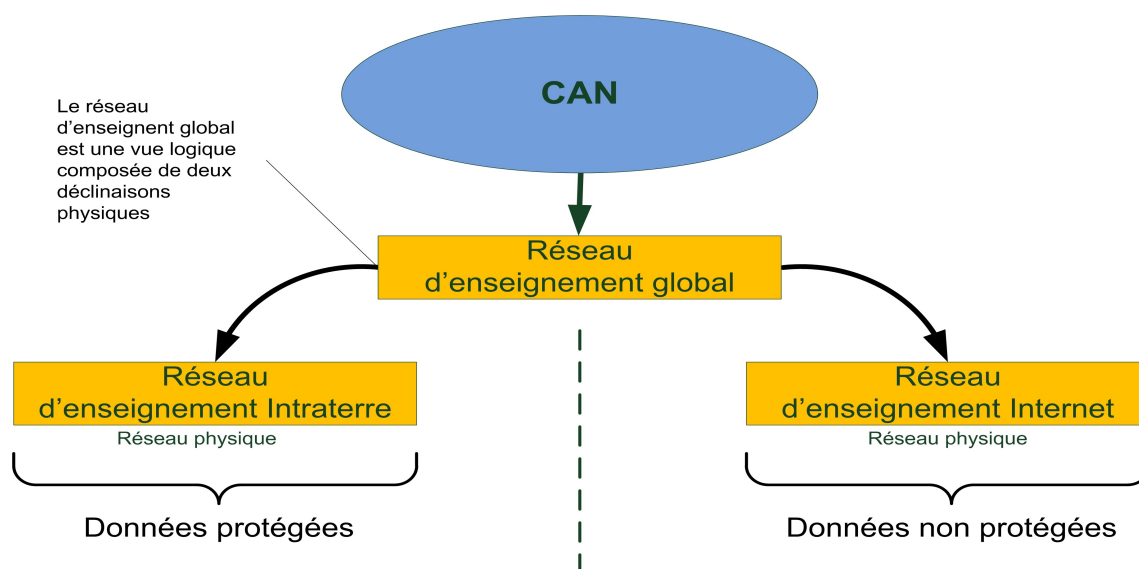


Illustration 9: Schéma de principe du réseau d'enseignement global

### 3.2.b) Le réseau d'enseignement Intraterre

Le réseau d'enseignement Intraterre est connecté au réseau intranet nommé « Intraterre ».

Le réseau Intraterre est **commun à tous les organismes de l'armée de terre**. Il est construit sur la base d'une infrastructure isolée de l'Internet afin de répondre aux contraintes de la PSIAT. En dehors de cet aspect, c'est un réseau classique qui propose des services bureautiques comme la messagerie, des sites web, des applications web ou des applications client/serveur.

L'administration et la maintenance de l'Intraterre sont confiées à la direction inter-armée des réseaux d'infrastructure et des systèmes d'information (DIRISI). La DIRISI se positionne en prestataire de service unique de la défense et l'ETRS n'a pas la possibilité d'intervenir directement sur les matériels du réseau Intraterre.

Les équipements actifs sont configurés pour un débit minimum de 100Mbits/sec et le lien entre les bâtiments permet de réaliser 10Gbits/sec. En revanche, l'infrastructure qui relie les organismes entre eux abaisse ce débit à une valeur proche de 8Mbits/sec. Toutefois, en 2013, ce débit sera multiplié par dix. Cette transformation a été actée officiellement dans le cadre d'une passation de marché.

Pour le moment, il n'existe pas encore d'espace numérique de travail en production sur le réseau d'enseignement Intraterre. A la date de rédaction de ce mémoire, une plate-forme de test est en cours de réalisation mais celle-ci n'est pas encore opérationnelle.

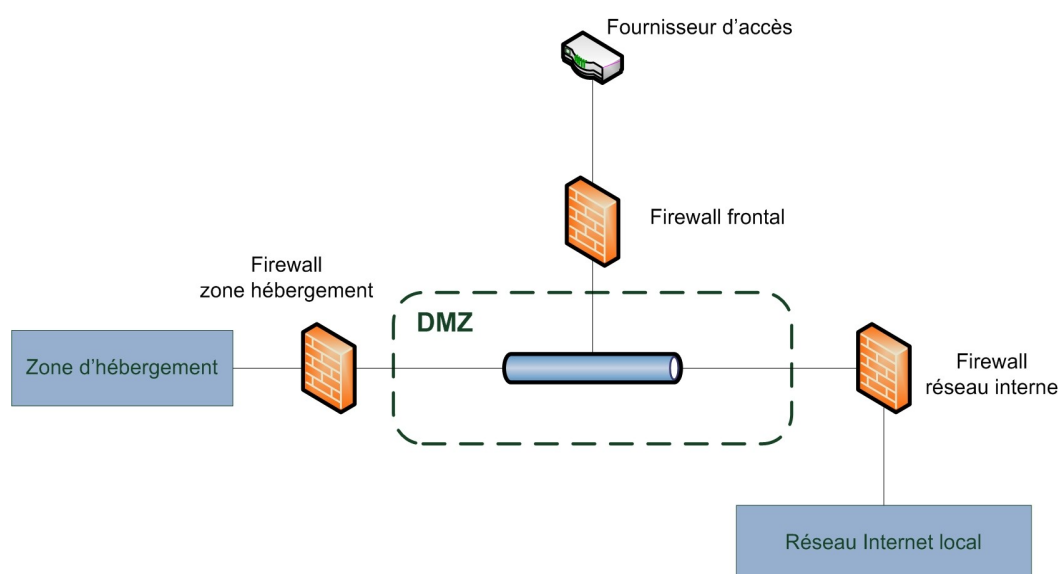
### 3.2.c) Le réseau d'enseignement Internet

Le réseau d'enseignement Internet est utilisé **conjointement** à son homologue connecté à l'Intraterre. L'implantation de l'Internet est beaucoup plus élevée que celle de l'Intraterre qui n'est présent que sur les sites de la Défense. A ce titre, la mise en œuvre du mode de partage de la connaissance en enseignement à distance sur le réseau Internet présente l'avantage de couvrir un territoire beaucoup plus vaste et donc de cibler un plus grand nombre d'apprenants. En revanche, les données qui circulent sur ce réseau ne doivent pas être classifiées, comme cela a été présenté dans les paragraphes précédents.

Les travaux de l'ETRS dans le domaine de l'enseignement à distance ont **majoritairement été réalisés sur le réseau d'enseignement connecté à l'Internet** car la stratégie initiale du projet CAN a toujours privilégié cette configuration en raison d'une politique d'ouverture globale et d'un souhait de délocalisation des cours maximum. C'est pourquoi aujourd'hui un espace numérique de travail est en production sur le réseau Internet alors qu'il n'est encore qu'en phase de développement sur le réseau Intraterre.

Le réseau Internet de l'ETRS est servi par une liaison « numéricâble compléte » professionnelle garantissant un débit de 20 Mbits/sec. L'administration et la gestion sont réalisées par le BFAO mais un accord de niveau de service souscrit avec le fournisseur garantit une intervention dans les 24 heures en cas de panne.

Comme le montre l'illustration ci-dessous, le schéma de principe du réseau Internet de l'école repose sur une architecture classique en zone démilitarisée (DMZ).



*Illustration 10: Schéma de principe de l'architecture Internet*

Un firewall frontal agit en coupure de réseau entre la ligne acheminée par le fournisseur d'accès et la zone à protéger, permettant ainsi un filtrage efficace des entrées/sorties. De plus, la zone d'hébergement et la zone de réseau Internet local sont implantées sur une infrastructure différente et sont protégées par un firewall.

Le firewall de la zone d'hébergement est configuré en portail captif et impose donc que les connexions soient authentifiées pour que le trafic soit autorisé. Cette restriction est indispensable car l'école n'a pas le contrôle des équipements utilisés par les stagiaires en chambre et doit donc être à même de journaliser toute l'activité.

### **3.2.d) Conséquences de l'existence de deux réseaux d'enseignement**

Nous avons vu que la mise en place de réseau d'enseignement Intraterre se justifie en raison des contraintes de la PSIAT et de l'existence de cours avec du contenu classifié. Le réseau Internet est utilisé car sa couverture géographique est beaucoup plus favorable à la mise en œuvre d'une politique d'enseignement à distance. Cette organisation **impose une scission nette du système d'information de la formation en deux parties distinctes et physiquement isolées.**

Le tableau ci-dessous présente les avantages et les inconvénients d'une telle organisation.

Avantages de 2 réseaux d'enseignement	Inconvénients de 2 réseaux d'enseignement
<ul style="list-style-type: none"> <li>- Confidentialité des cours améliorée,</li> <li>- Contrôle du support de diffusion de l'information en fonction de sa classification,</li> <li>- Absence de risque d'exposition de données classifiées sur l'Internet sans authentification.</li> <li>- Services différents adaptés aux réseaux.</li> </ul>	<ul style="list-style-type: none"> <li>- Redondance de moyens matériels, humains et de services pour l'administration et l'exploitation,</li> <li>- Complexité multi plate-forme de l'architecture et de l'accès,</li> <li>- Règles de gestion différentes d'un réseau à l'autre,</li> <li>- Caractéristiques très hétérogènes (débit, bande passante etc.)</li> </ul>

*Tableau 2: Avantages et inconvénients de deux réseaux d'enseignement isolés*

En synthèse du tableau, il faut retenir que l'existence de deux réseaux d'enseignement physiques permet une stricte séparation des données en fonction de leur classification et que cette architecture présente des caractéristiques de sécurité élevée pour ce type de système.

Un inconvénient majeur ressort toutefois de cette organisation. L'existence de deux entités autonomes **alourdit la charge de gestion** des équipements, provoque des **effets de redondance** et **complexifie les règles de gestion** du SIF.

*Le Campus Area Network, ou CAN, désigne l'infrastructure sur laquelle repose le réseau d'enseignement global en charge de l'acheminement des ressources informatiques nécessaires au fonctionnement des services métiers et des modes de partage de la connaissance.*

*Le réseau d'enseignement global est une entité logique utile pour une vision dont le niveau d'abstraction est de portée globale à l'école. Dans les faits, ce réseau d'enseignement est constitué de deux réseaux d'enseignement physique connectés pour l'un à l'Internet et l'autre à l'Intranet, un intranet spécifique à l'armée de Terre habilité à traiter des données classifiées.*



### 3.3 : Les zones d'implantation géographiques du SIF

Les principes de fonctionnement et de gestion d'un système d'information sont généralement impactés par la localisation des éléments qui le composent. Le système d'information de la formation n'échappe pas à cette règle.

Pour bien comprendre les références géographiques qui seront formulées dans la suite de ce mémoire, la partie ci-dessous présente les différentes zones d'implantation du SIF dans l'enceinte de l'école.

Comme le présente l'illustration ci-dessous, il existe trois zones majeures d'implantation du SIF à l'école : La zone des plates-formes d'instruction, la zone hébergement et la zone cadre.



Illustration 11: Situation géographique du système d'information de la formation

La zone des plates-formes d'instructions (PFI) est matérialisée par les bâtiments qui permettent d'exécuter les services métier rattachés au mode de partage de la connaissance en présentiel. Il s'agit par exemple des salles de cours ou des salles de travaux dirigés. La population dominante est constituée de formateurs et de stagiaires. La zone des PFI représente le centre névralgique pédagogique de l'école car la majorité des formations se déroulent en son sein. La disponibilité des



services du SIF y est critique car l'interruption d'un outil ou d'une fonctionnalité peut avoir un impact considérable sur le planning d'un stage, a fortiori lorsque celui-ci est de courte durée.

Historiquement, la zone des PFI était exclusivement reliée au réseau d'enseignement connecté à l'Intraterre. Depuis 2008, la stratégie de développement de l'enseignement numérique de l'école a conduit à migrer sur le réseau d'enseignement Internet une quinzaine de salles de cours sur la soixantaine recensée afin de les relier à l'espace numérique de travail en production sur ce réseau.

La zone d'hébergement est matérialisée par les bâtiments des stagiaires et représente 600 chambres. Actuellement, 300 de ces chambres sont équipées d'une connexion au réseau d'enseignement Internet proposée gratuitement aux résidents dans le but de leur faciliter l'accès à la connaissance. A la fin de l'année 2011, toutes les chambres seront équipées. La disponibilité de cette connexion réseau est importante mais non critique car il existe d'autres points d'accès au réseau Internet dans les salles de cours ou au centre de documentation. De plus, la zone n'est pas occupée en journée car la population dominante est dans la zone des PFI durant les heures ouvrables.

La zone cadre est matérialisée par les bâtiments qui regroupent les directions et les bureaux au service de l'administration générale et de la gestion de l'école. La population dominante de cette zone est constituée du personnel affecté pour emploi que l'on désigne par le terme « permanent ».

La zone cadre est reliée aux deux réseaux d'enseignement de l'école et la majeure partie des bureaux de ce quartier dispose de deux postes de travail connecté chacun à un réseau différent. La disponibilité des services du SIF est importante mais non critique dans ce secteur car la nature administrative des tâches qui s'y déroulent relève rarement d'un caractère d'urgence.

Enfin, le bureau de formation assistée par ordinateur (BFAO), situé dans les locaux de la zone cadre, contient le personnel et le matériel qui permettent d'assurer les servitudes en ressources informatiques du SIF et de les distribuer aux différentes zones de l'école via les réseaux d'enseignement. Les tâches qui y sont exécutées relèvent principalement de l'administration réseau et de la maintenance. La population présente est strictement composée du personnel dont le domaine d'emploi évolue autour de l'informatique.

*Le système d'information de la formation est implantée dans l'enceinte de l'école sur trois zones majeures : la zone d'hébergement correspondant aux chambres des stagiaires, la zone des plates-formes d'instruction (PFI) matérialisée par les salles de cours et la zone cadre où se déroule les tâches administratives annexes.*

*Le bureau de formation assistée par ordinateur (BFAO), responsable de la mise en œuvre des éléments participant à la servitudes des ressources informatiques est lui aussi intégré à la zone cadre.*

### 3.4 : Réduction de périmètre technique du projet CNAM

*Les éléments présentés depuis le début de ce chapitre font ressortir que le système d'information de la formation est une structure complexe qui repose sur une infrastructure conséquente pour le mettre en œuvre. La prise en compte de deux réseaux d'enseignement physiques pour former un seul réseau d'enseignement global est l'une des raisons majeures justifiant cette complexité..*

*Pour mieux définir le contexte dans lequel prend sa place ce mémoire CNAM, la partie ci-dessous fixe une réduction de périmètre à l'environnement technique dans lequel s'intègre le projet.*

Nous avons vu que l'infrastructure technique qui fournit les ressources informatiques nécessaires au fonctionnement du système d'information de la formation est notamment représentée par le Campus Area Network, ou CAN, et son réseau d'enseignement global. Le réseau d'enseignement global est une vue logique qui se matérialise en fait par deux réseaux d'enseignement physiques installés pour l'un sur le réseau Internet et pour l'autre sur l'intranet de l'armée de Terre : l'Intraterre.

Nous savons également que l'état d'avancement des travaux de l'ETRS dans le domaine de l'enseignement numérique n'est pas égal selon le réseau d'enseignement physique considéré. Actuellement, c'est le réseau Internet qui concentre le plus d'attention et les actions réalisées sur ce dernier permettent aujourd'hui la mise en œuvre d'un espace numérique de travail productif.

Enfin, le réseau Internet a été choisi en raison de sa capacité à dépasser les limitations de couverture du réseau Intraterre et à favoriser ainsi la délocalisation des cours. D'un point de vue technique, ce réseau présente également un avantage supplémentaire par rapport à son homologue intranet. En effet, l'administration et la gestion des équipements informatiques connectés au réseau Internet sont encore sous la responsabilité de l'ETRS alors que c'est la direction inter-armée des réseaux d'infrastructure et des systèmes d'information (DIRISI) qui s'occupent de ces tâches pour le réseau Intraterre. De ce fait, la capacité à concevoir et mettre en œuvre des architectures informatiques personnalisées et adaptées à ses besoins est beaucoup plus importante pour l'ETRS sur le réseau Internet que sur l'Intraterre.

En accord avec l'Officier Management des Systèmes d'Information (OMSI) de l'école, M. Martineau, et en référence aux éléments de comparaison des paragraphes précédents qui portent sur l'état d'avancement des travaux et sur la capacité d'action, il a été décidé d'appliquer une réduction au périmètre technique de mon projet CNAM.

Dorénavant, seules les problématiques de diffusion des flux pédagogiques multimédias qui circulent sur **le réseau d'enseignement connecté à l'Internet seront traitées et le réseau Intraterre ne sera plus pris en compte**. Cette réduction de périmètre prend effet immédiatement et s'appliquera à la définition du besoin mais aussi à la conception et la réalisation des solutions qui permettent d'y répondre.

*Le réseau d'enseignement global du Campus Area Network se décline en deux réseaux d'enseignement physiques connectés à l'Internet et au réseau Intraterre.*

*Ce mémoire applique une réduction validée officiellement au périmètre technique de ce projet CNAM et ne traitera plus, dorénavant, que de la diffusion des flux multimédias pédagogiques acheminés par le réseau d'enseignement connecté à l'Internet.*

## 3.5 : L'espace numérique de travail

*L'espace numérique de travail (ENT) connecté au réseau d'enseignement Internet est au cœur de la stratégie de développement de l'enseignement numérique de l'ETRS car c'est lui qui représente et matérialise le mieux la majeure partie des actions qui ont pu être effectuées dans ce domaine.*

*Une bonne appréhension de l'espace numérique de travail de l'école est indispensable à la compréhension globale du projet CNAM. Pour cela, la partie qui suit propose dans un premier temps une présentation générale de l'ENT et fournit ensuite une analyse plus détaillée en respectant une approche selon les processus du référentiel de bonnes pratiques ITIL V3.*

### 3.5.a) Présentation générale de l'espace numérique de travail

Un espace numérique de travail (ENT) est un système qui centralise en un point d'accès unique et sécurisé des services à vocation pédagogique. L'objectif est d'accompagner les utilisateurs, tels des apprenants ou des formateurs, en leur proposant des fonctionnalités qui permettent d'organiser leur travail et faciliter le partage de la connaissance.

Ce type de système se présente généralement sous la forme d'un **portail applicatif** à laquelle on accède depuis un navigateur. Son principal atout réside dans sa capacité à présenter dans une seule page web la concaténation de plusieurs services et fonctionnalités hébergés sur des serveurs web différents. Grâce à un **système d'authentification centralisée**, les services se partagent les mêmes informations d'identification saisies une seule fois par l'utilisateur lors de sa connexion initiale. Ce type de mécanisme, nommé « Single Sign-On » (SSO), permet d'ajouter à volonté des nouveaux services dans l'ENT sans exiger de nouvelle phase d'authentification lors de leur utilisation.

Le socle technique nécessaire à la mise en œuvre d'un espace numérique de travail est complexe. En effet, des services transverses supplémentaires de base de données, d'annuaire d'utilisateurs, de messagerie, de stockage partagé ou de génération dynamique de pages web sont nécessaires à son exploitation. A titre d'exemple, on recense une quarantaine de serveurs virtualisés pour faire fonctionner l'espace numérique de travail de l'école.

L'espace numérique de travail de l'école des transmissions répond à la description générale effectuée ci-dessus. Le produit utilisé repose sur le projet ESUP portail (<http://www.esup-portail.org>) qui est déjà utilisé par une quarantaine d'universités et de centres de recherche française.

### 3.5.b) Présentation de l'ENT d'après les processus ITIL

La démarche ITIL est un recueil de bonnes pratiques destinées à améliorer la qualité des systèmes d'information en proposant une approche selon quatre phases qui couvrent la stratégie, la conception, la transition et l'exploitation des services. Pour chacune de ces phases, des sous-processus destinés à des problématiques spécifiques peuvent s'appliquer. L'exécution de chaque processus et sous-processus n'est pas systématique et dépend du contexte de réalisation du projet. Une présentation générale de la démarche ITIL est fournie en annexe 2.

Le projet CAN et sa partie en charge de l'espace numérique de travail se calquent sur le recueil de bonnes pratiques ITIL. Cette organisation a été mise en place par M. Martineau afin de définir une structure de conduite de projet efficace. Bien sûr, modéliser et présenter un processus global de conception ou d'exploitation englobant tout l'espace numérique de travail est difficile. Une telle

démarche à beaucoup plus de chance d'aboutir si elle s'applique à chacun des services de l'ENT. Pourtant, à chacun des niveaux d'abstraction d'un projet, la démarche ITIL est applicable et permet de guider les équipes en charge de la conduite.

Les paragraphes ci-dessous présentent les phases de base de la démarche ITIL applicables au niveau de l'espace numérique de travail. Seules la stratégie, la conception et l'exploitation sont traitées. La transition n'est pas abordée car l'ENT s'est intégré dans un contexte nouveau qui n'a pas nécessité de prendre en compte cet aspect.

### **- La stratégie**

L'énumération des fonctionnalités proposées par un système d'information est une bonne façon de refléter la politique choisie pour piloter son développement. Dans cet esprit, la démarche ITIL préconise d'entretenir un document nommé « portefeuille de services ». Ce document est utilisé pour définir la stratégie vers laquelle s'oriente un projet et sert de support au processus de conception des services.

Le tableau ci-dessous présente la liste des éléments inscrits au portefeuille de services du projet CAN/ENT<sup>9</sup>. Il reflète la stratégie globale appliquée au projet. Les éléments recensés témoignent de la volonté générale de proposer aux utilisateurs un accès sécurisé vers des fonctionnalités qui permettent de partager les connaissances et de les assister dans l'organisation de leur travail.

---

<sup>9</sup> Le portefeuille de services du projet CAN/ENT est fourni en annexe 1

Nom du service	Description
Accès et authentification	Couvre l'aspect physique, logique et la sécurisation du réseau d'enseignement.
Messagerie	Fonctionnalité de mail
Emploi du temps en ligne	Permet la consultation des emplois du temps de stagiaire et de formateur
Cours en ligne	Consultation en ligne de supports de cours convertis au format numérique
Référencement des ressources SIC	Accès indexé aux ressources pédagogiques
Ticket d'incident	Déclaration et prise en compte des incidents
TV en ligne	Consultation en zone d'hébergement de chaînes de TV numérique dans un navigateur.
Forum professionnel	Forum de discussion
Espace de stockage utilisateur	Lecture et écriture de fichier dans un espace de stockage personnel accessible par le web
Liste de diffusion	Envoyer des mails à plusieurs destinataires avec une seule adresse
Annuaire	Consultation des coordonnées d'un stagiaire ou d'un formateur
Chaîne éditoriale	Publication contrôlée et versionnée de document
Générateur de QCM	Contrôle de connaissances en ligne

Tableau 3: Le portefeuille de services du projet CAN/ENT

### **- La conception**

La conception d'un service selon la démarche ITIL prend en compte la sécurisation des éléments. A un niveau global à l'ENT, il a été défini par l'équipe en charge du projet que les accès aux services de l'espace numérique de travail **doivent tous être protégés par une phase d'authentification**. Pour éviter aux utilisateurs de s'authentifier à chaque fois qu'ils utilisent un service différent, une centrale d'authentification sécurisée (SSO) a été mise en place pour partager les informations de connexion. Cette organisation permet de dégager une règle de gestion globale au projet ENT qui précise que tous les services doivent intégrer, **dès la conception**, la prise en compte de ce partage d'authentification. Cette règle de gestion est à intégrer dans la phase de conception des solutions qui seront proposées dans le cadre de ce projet CNAM.

D'autres processus ITIL à initier lors de la phase de conception des services ont également été traités à un niveau global à celui du projet CAN/ENT.

Par exemple, la capacité a été gérée en identifiant pour chaque élément du portefeuille de services le nom de son propriétaire fonctionnel et les compétences nécessaires à la mise en œuvre. La prise en compte de ce type d'information améliore notamment la gestion des ressources humaines affectées à un services. Pour le portefeuille de services de l'ENT, il ressort que les éléments sont confiés au BFAO et au BENS et que les compétences nécessaires sont d'ordre technique et pédagogique.

Enfin, la continuité technique des services et la gestion de leur disponibilité ont également été traitées à un niveau global au projet CAN/ENT. L'une des actions de ces processus a consisté à souscrire un contrat de service avec le fournisseur d'accès Internet qui alimente le réseau d'enseignement correspondant de l'école. Ce contrat de service stipule un délai d'intervention inférieur à 24 heures en cas d'indisponibilité. La gestion de la continuité et de la disponibilité des solutions réalisées dans le cadre du projet CNAM doit prendre en compte cette caractéristique de niveau global et s'efforcer de mettre en œuvre des plans d'action qui permettent de recouvrir à un fonctionnement nominal dans un délai lui aussi inférieur à 24 heures en cas de dysfonctionnement.

### **- L'exploitation**

La démarche ITIL préconise de traiter la gestion des incidents et des problèmes durant l'exploitation des services. Ces aspects sont pris en compte au niveau du projet CAN/ENT par une cellule du BFAO dédiée à l'exploitation. Les utilisateurs peuvent informer d'un dysfonctionnement par téléphone ou en utilisant un service de saisie de ticket d'incident intégré à l'ENT.

*L'espace numérique de travail est un portail applicatif de type web qui permet un accès unique et sécurisé à des services destinés à faciliter l'organisation du travail et le partage de la connaissance. Le socle mis en place à l'École des transmissions s'appuie sur le projet ESUP portail déjà en cours d'utilisation dans une quarantaine d'universités et centres de recherche français.*

*Le projet CAN/ENT est géré en se référant au recueil de bonnes pratiques ITIL qui offre une assistance dans la phase de définition de la stratégie, de conception, de transition et d'exploitation des services. La démarche ITIL couvre tous les aspects du cycle de vie d'un service. Son application à l'espace numérique de travail a permis d'anticiper et de gérer des aspects plus facilement ignorés dans le cadre d'une démarche classique. Le projet CNAM qui motive ce mémoire se calque lui aussi sur la démarche ITIL.*

## **3.6 : Les types de médias proposés par l'ENT**

*Les services de l'espace numérique de travail ont vocation à proposer l'accès à des ressources pédagogiques numériques. Pour l'utilisateur, ces ressources se matérialisent par des documentations en ligne, des pages web interactives ou des supports de cours numérisés qui peuvent être enrichies selon les cas de médias de type audio ou vidéo, tels la restitution filmée d'une séance de cours ou la démonstration de l'utilisation d'un matériel.*

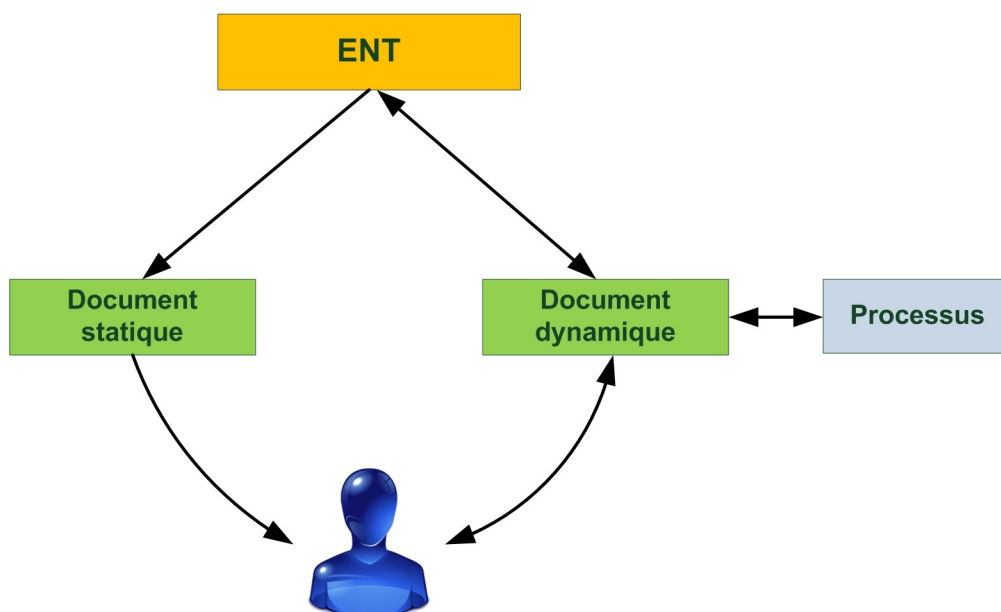
*La partie ci-dessous présente les différents types de ressources pédagogiques proposées par l'espace numérique de travail. L'étude est effectuée selon trois approches différentes fondées soit sur le type de document mis en jeu, soit sur les technologies de développement utilisées, soit sur les types de serveurs utilisés pour l'hébergement.*

### **3.6.a) L'approche document**

Il existe deux catégories de documents disponibles sur l'espace numérique de travail.

La première catégorie comprend **les ressources « statiques »**. Il s'agit de documents, d'images, de sons ou de vidéos disponibles au téléchargement ou intégrées dans des pages web. Ces ressources sont statiques car leur contenu est figé et elles se présentent toujours sous la même forme à tous les utilisateurs, quel que soit l'heure ou le lieu de consultation.

La seconde catégorie comprend les **ressources « dynamiques »**. Ces ressources sont dynamiques car elles permettent une grande interaction avec l'utilisateur et leur forme peut varier dans le temps. Typiquement, il s'agit des modules d'enseignement à distance dont le contenu s'adapte en fonction des réponses d'un stagiaire ou de son état d'avancement dans un parcours de formation.



*Illustration 12: Type de média selon l'approche document*

Comme le montre l'illustration ci-dessus, le lien entre un document statique et l'utilisateur est toujours unidirectionnel car il n'y a pas de possibilité d'interaction. En revanche, le lien avec un document dynamique est bidirectionnel car ce type de document se présente dans un contexte qui introduit des processus permettant des interactions avec l'utilisateur.

### **3.6.b) L'approche développeur**

Les technologies employées pour créer les ressources pédagogiques de l'espace numérique de travail sont de deux types.

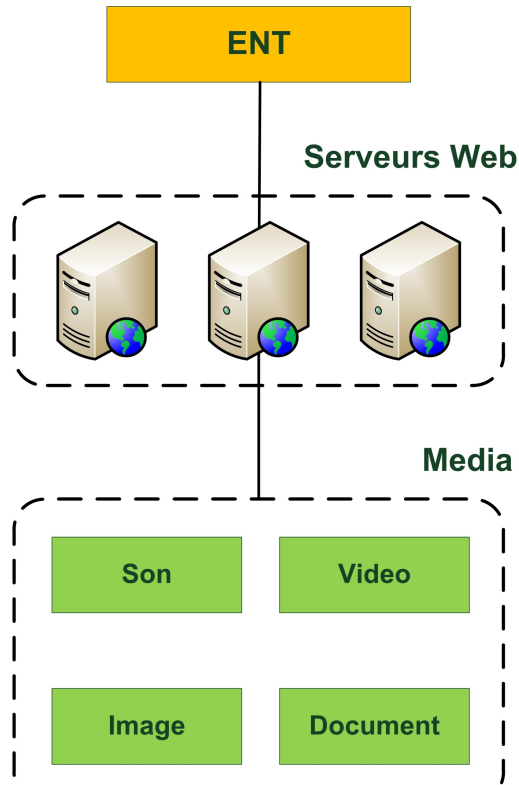
Pour les ressources statiques, les outils employés sont ceux proposés par les suites bureautiques classiques. Accessoirement, des outils de création web peuvent être utilisés pour construire des pages simples proposant du texte, des images ou des liens vers d'autres ressources.

Les ressources dynamiques utilisent les technologies de client riche, type Adobe Flash ou Microsoft Silverlight, et nécessitent l'installation d'un composant additionnel dans le navigateur des postes clients.

Les compétences nécessaires pour développer des ressources dynamiques utilisant ce type de technologie nécessitent de bonnes connaissances dans les domaines de l'audio, la vidéo et la programmation. L'école ne développe pas ses composants d'enseignement à distance reposant sur l'utilisation de ressources dynamiques mais sous-traite leur acquisition à des sociétés spécialisées.

### 3.6.c) L'approche serveur

Les utilisateurs accèdent aux ressources pédagogiques de l'espace numérique de travail à l'aide d'un navigateur. Pour assurer cette liaison, des serveurs sont nécessaires pour prendre en charge la distribution des éléments correspondants.



*Illustration 13: Type de média selon l'approche serveur*

Comme le présente l'illustration ci-dessus, les médias proposés par l'ENT sont exclusivement hébergés et diffusés par des serveurs web. Ce type de serveur se prête bien à la transmission des ressources statiques types pages web ou documents de bureautique. En revanche, leur utilisation pour la diffusion de média type son ou vidéo n'est pas optimale et n'offre qu'une qualité de service moyenne pour l'utilisateur final. Ce constat est à la base de la définition du besoin qui motive ce mémoire et justifie la volonté de mettre en place une solution de diffusion des flux pédagogiques multimédias, comme cela sera présenté lors de l'étude du besoin au prochain chapitre.

*Les ressources pédagogiques proposées par l'espace numérique de travail sont des documents de bureautique classiques, des sons, des images, des vidéos ou des programmes compilés qui s'exécutent dans un client riche. Ces ressources sont soit statiques, c'est à dire figées et toujours présentées sous la même forme, soit dynamiques et capables d'interagir fortement avec l'utilisateur et de varier dans le temps.*

*La transmission des ressources pédagogiques jusqu'au client est exclusivement prise en charge par des serveurs web. Ces serveurs sont bien adaptés à l'exploitation de ressources statiques mais ils sont moins performant dans le cas de sons ou de vidéos.*



*Dans ce chapitre, nous avons vu que le système d'information de la formation (SIF) est l'outil de production qui permet le partage et la transmission des connaissances à l'École des transmissions. Son modèle de fonctionnement met en œuvre des clients qui accèdent à des services métiers à vocation pédagogique par l'intermédiaire de différents modes de partage de la connaissance, tel le mode présentiel ou l'enseignement à distance.*

*Pour fonctionner, les modes de partage de la connaissance et les services métiers consomment des ressources matérielles, informatiques, pédagogiques et humaines fournies par l'infrastructure du système d'information de la formation. Ces ressources transitent par des canaux d'acheminement différents selon le type mis en jeu.*

*Le Campus Area Network (CAN) et l'espace numérique de travail (ENT) sont des éléments constitutifs du système d'information de la formation.*

*Le CAN désigne les canaux d'acheminement qui participent au transfert des ressources informatiques et des ressources pédagogiques numériques. Il forme le réseau d'enseignement global composé de deux réseaux d'enseignement physiques connecté l'un à l'Internet et l'autre à un intranet.*

*L'espace numérique de travail désigne un portail web qui centralise et sécurise l'accès à des services métier facilitant l'organisation du travail et le partage de la connaissance. Parce qu'il existe deux réseaux d'enseignement physiques, l'ETRS a la capacité de mettre en œuvre deux espace numérique de travail. Une réduction de périmètre technique validée par le directeur des systèmes d'information précise toutefois que le projet CNAM qui motive ce mémoire ne traite que de l'espace numérique de travail connecté à l'Internet.*

## 4 : ÉTUDE DU BESOIN

*Les études de l'existant des deux chapitres précédents ont permis de définir le contexte fonctionnel et technique dans lequel évolue ce projet CNAM. Ce chapitre s'attache cette fois à présenter le besoin auquel le projet doit répondre.*

*Pour cela, une première partie expose la situation et le constat à l'origine des problèmes rencontrés. Une seconde partie exprime ensuite la formulation de l'expression du besoin en présentant les fonctionnalités souhaitées, les contraintes et les exigences.*

### 4.1 : Le constat à l'origine du besoin

*Les objectifs de ce projet CNAM ne peuvent être clairement appréhendés sans une vision précise des problèmes à résoudre. A cet effet, la partie ci-dessous présente la situation et le constat à l'origine de l'expression de besoin du projet.*

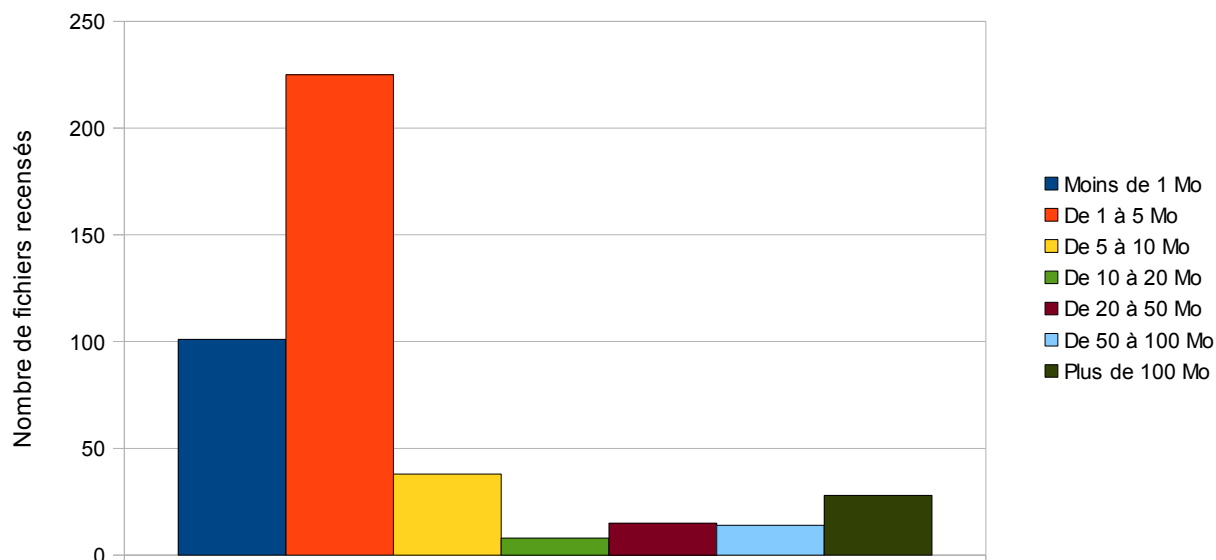
L'expression de besoin qui motive ce mémoire s'appuie sur un constat formulé à partir d'une situation clairement identifiée et reproductible qui met en jeu des acteurs et un contexte définis. Les acteurs sont représentés par l'espace numérique de travail, les utilisateurs et leur navigateur Internet. Le contexte à reproduire est obtenu lorsque ces utilisateurs accèdent à l'espace numérique de travail à l'aide de leur navigateur et consultent des ressources pédagogiques du service de cours en ligne.

Lorsque ces utilisateurs se retrouvent dans le contexte énoncé précédemment, l'affichage de ressources pédagogiques statiques de type document bureautique ou page web est immédiat dans le navigateur. En revanche, si l'une des ressources intègre un média, la consultation de ce dernier est soumise à un **temps de latence** et sa restitution globale est **saccadée quels que soient l'heure et le lieu d'accès**. Par exemple, lorsqu'un stagiaire accède à une page web de documentation qui contient une vidéo, la page s'affiche instantanément dans le navigateur mais la vidéo, elle, n'est accessible qu'après une période d'attente variable et sa visualisation est discontinue. Ce constat nuit à la qualité générale de l'espace numérique de travail et plus particulièrement au confort pédagogique des apprenants qui consultent le service de cours en ligne. Par extension, c'est la popularité et la pérennité du mode de partage de la connaissance basé sur l'enseignement à distance qui est mis en jeu.

Les médias proposés par le service de cours en ligne sont des vidéos filmées durant des séances de formation. Un recensement que j'ai réalisé sur le serveur en charge de l'hébergement des fichiers correspondants révèle un total de 429 éléments pour un volume global de 9Go. La taille de chacun des éléments est comptabilisée dans le tableau n°4 et le graphique n°14 ci-dessous.

Taille	Moins de 1Mo	De 1 à 5 Mo	De 5 à 10 Mo	De 10 à 20 Mo	De 20 à 50 Mo	De 50 à 100 Mo	Plus de 100 Mo
Fichiers	101	225	38	8	15	14	28

Tableau 4: Tableau de répartition des tailles de fichier vidéo du service de cours en ligne

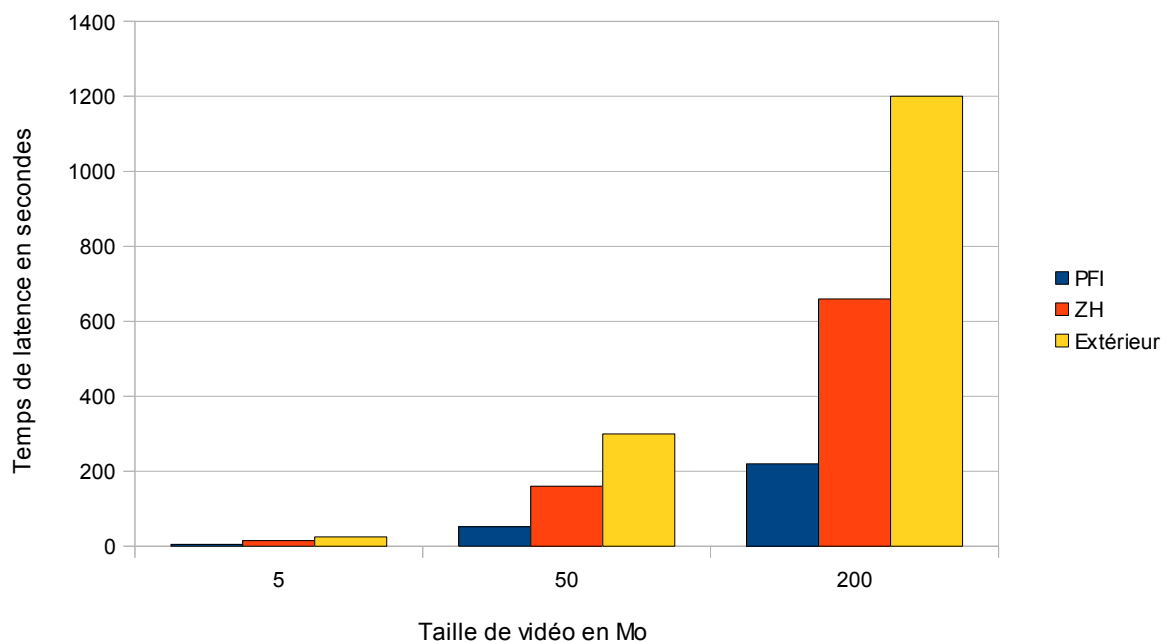


*Illustration 14: Graphique de répartition des tailles de fichier vidéo*

L'étude de la répartition des tailles de fichier fait apparaître qu'environ 75% des vidéos proposées par le service de cours en ligne ont une taille inférieure à 5Mo. En revanche, parmi les 25% restants, 15% des fichiers ont une taille supérieure ou égale à 20 Mo et celle-ci peut parfois dépasser la centaine de Mo. Globalement, ces chiffres me permettent d'indiquer que si la majeure partie des vidéos diffusées sont de petite taille, il existe aussi un nombre non négligeable de fichiers de taille conséquente.

Pour compléter mon analyse, j'ai procédé à des mesures de temps de chargement qui montrent que la durée initiale du temps de latence observé avant le démarrage d'une vidéo intégrée dans une ressource pédagogique est directement liée à la taille du fichier associé et à la zone dans laquelle se situe l'utilisateur. Ces mesures s'appuient sur un test qui met en œuvre trois pages web statiques incluant chacune une vidéo différente de taille égale à soit 5, 50 ou 200Mo. J'ai choisi ces tailles car elles représentent bien les ordres de grandeurs révélés par l'étude de répartition présentée précédemment. Pour chaque accès à l'une des pages web, le temps d'attente avant le début de la vidéo a été chronométré. Les mesures ont été effectuées depuis la zone des plates-formes d'instruction (PFI), la zone d'hébergement (ZH) et l'extérieur de l'école afin de refléter les différents cas d'utilisation possibles du service de cours en ligne.

Comme cela a été dit, le résultat des mesures, illustré par le graphique n°15, indique clairement que le temps d'attente avant la visualisation d'une vidéo est impacté par la taille de son fichier et la localisation de l'utilisateur. Alors que le temps d'accès à une vidéo est de quelques secondes quelle que soit sa taille lorsque le test est réalisé en zone PFI, la durée s'exprime en dizaine de secondes depuis la zone d'hébergement et en centaines de secondes lorsque la connexion a lieu depuis l'extérieur de l'école. Ces différences de durée sont liées à l'architecture technique du réseau Internet de l'école et aux différents firewalls et éléments actifs que les données doivent traverser selon la localisation de leur destinataire.



*Illustration 15: Évolution moyenne du temps de latence avant accès à une vidéo*

Dans les faits, **un stagiaire qui accède à une vidéo depuis l'extérieur de l'école subira un temps d'accès plus important que si la connexion a lieu depuis la zone des PFI**. Cette situation est contradictoire vis à vis de la stratégie de développement de l'enseignement à distance de l'école et de son ambition à délocaliser les parcours de formation. En effet, **la zone des PFI est naturellement dédiée au mode de partage de la connaissance en présentiel** alors que **l'enseignement à distance est destiné à être mis en œuvre à l'extérieur de l'école**. C'est ce constat qui est à l'origine de l'expression de besoin qui motive ce mémoire CNAM.

*Le service de cours en ligne de l'espace numérique de travail expose des ressources pédagogiques statiques de type page web ou document de bureautique parfois enrichies d'une ou plusieurs vidéos. Lorsqu'un utilisateur accède à ce type de ressource pédagogique enrichie d'un média, le document s'affiche instantanément dans le navigateur. En revanche, la vidéo ne débute qu'après un temps de latence proportionnel à la taille du fichier associé et croissant selon que l'utilisateur se situe dans la zone des plates-formes d'instruction, la zone d'hébergement ou l'extérieur de l'école. Enfin, une fois démarrée, la visualisation de la vidéo est généralement saccadée et discontinuée.*

*Ce constat est à l'origine de l'expression de besoin qui motive ce mémoire CNAM. La situation actuelle est en effet incompatible avec la volonté de l'École des transmissions à délocaliser ses parcours de formation en les exportant à l'extérieur de son enceinte grâce au mode de partage de la connaissance basé sur l'enseignement à distance.*

## 4.2 : L'expression du besoin

*Les conséquences du constat présenté dans la partie précédente nuisent fortement à la pérennité du service de cours en ligne et à l'espace numérique de travail. C'est pour remédier à cette situation qu'une expression de besoin a été initialisée et prise en compte dans le cadre de ce projet CNAM. Sa formulation s'articule autour de trois points présentés ci-dessous qui traitent des fonctionnalités souhaitées, des contraintes à prendre en compte et des exigences.*

Le temps de latence observé lors de l'accès à un média intégré dans une ressource pédagogique du service de cours en ligne et le manque de fluidité durant sa consultation sont à l'origine de l'expression de besoin sur laquelle repose ce mémoire. La formulation du besoin a été exprimée par M. Martineau, officier en management du système d'information (OMSI) de l'École des transmissions et tuteur entreprise de ce projet CNAM.

### 4.2.a) Les fonctionnalités souhaitées

La solution à mettre en œuvre dans le cadre du projet doit permettre de diminuer, voire annuler, le temps de latence observé lors de l'accès à un média intégré dans une ressource pédagogique du service de cours en ligne. Quels que soit l'heure et le lieu de consultation, un utilisateur doit en effet pouvoir consulter un média sans subir le temps d'attente actuellement imposé. De plus, la restitution doit être fluide et l'utilisateur doit pouvoir se déplacer au sein de la plage de consultation du média afin d'avancer ou revenir en arrière et accéder ainsi à une portion donnée. Ce type de comportement est possible et se rencontre fréquemment sur les sites Internet qui proposent la consultation de contenus en ligne, tels les sites de vidéos partagées Youtube (<http://www.youtube.fr>) ou DailyMotion (<http://www.dailymotion.fr>).

A un niveau supérieur, l'objectif à atteindre consiste à disposer d'une plate-forme qui ne limite pas l'utilisation et l'intégration de média dans les ressources pédagogiques en raison de performances insuffisantes lors de la consultation.

Pour l'École des transmissions, il est impératif d'assurer l'équité des conditions d'enseignement pour les stagiaires et cela quel que soit le mode de formation choisi. Pourtant, alors qu'en mode présentiel le contrôle de l'environnement, du matériel et des configurations est total, rien ne garantit qu'il en soit de même pour les élèves en formation à distance.

Les enjeux qui reposent sur le service de cours en ligne visent donc à ne pas faire de discrimination entre le mode de partage de la connaissance en présentiel et à distance en maintenant l'envie d'apprendre et en diffusant une bonne image de l'enseignement à distance. C'est pourquoi l'amélioration de la qualité de service de consultation des flux multimédias constitue un facteur de réussite important dans l'adoption globale de l'espace numérique de travail.

### 4.2.b) Les contraintes

Les contraintes imposées par l'expression du besoin portent sur deux aspects.

La solution à mettre en œuvre doit permettre de faire face à un **scénario de référence** représentatif d'une situation où l'exploitation de l'espace numérique de travail est élevée. Ce scénario, **validé par M. Martineau**, correspond à la montée en charge provoquée par 200 utilisateurs connectés au service de cours en ligne qui consultent simultanément un média référencé dans une ressource pédagogique. Ce média peut être différent pour chaque utilisateur, seule compte la **capacité à pouvoir supporter au même moment 200 utilisateurs différents souhaitant accéder à un**

**média quelconque.** Un tel scénario est par exemple envisageable dans le cadre de révisions communes préalables à un contrôle de connaissance en ligne auxquelles seraient inscrites de nombreuses personnes.

Enfin, d'un point de vue technique, la solution mise en œuvre doit être opérationnelle même au sein d'un **réseau informatique à faible débit dont la bande passante ne dépasse pas 128 Kbit/sec.** Cette contrainte limitative se justifie en effet par la nécessité de pouvoir proposer un accès à l'espace numérique de travail même aux personnels déployés sur un théâtre d'opération extérieure. L'expérience montre que sur certains de ces théâtres, les capacités techniques des liaisons mises en œuvre permettent difficilement d'envisager un débit supérieur.

#### 4.2.c) Les exigences

D'un point de vue fonctionnel, l'expression de besoin stipule que la solution à concevoir doit s'intégrer avec un couplage faible vis à vis de l'existant. Cette exigence signifie que les modifications à apporter pour intégrer la nouvelle solution doivent être minimales. Par exemple, la solution doit permettre d'utiliser les vidéos existantes du service de cours en ligne sans nécessiter une nouvelle phase de production. Cet aspect n'exclut pas une éventuelle conversion des médias mais cette étape devra alors rester transparente vis à vis des équipes fonctionnelles.

De plus, au sein des cours en ligne, seuls les liens pointant vers des vidéos pourront être modifiés. En aucun cas, la mise en place de la solution ne doit provoquer d'incompatibilité qui nécessite une réécriture complète des ressources pédagogiques.

Ces exigences sont formulées dans le but d'éviter une interruption du service de cours en ligne et de limiter les coûts en concevant une solution qui nécessite des modifications trop nombreuses à apporter à l'existant.

#### 4.2.d) Synthèse de l'expression du besoin

Fonctionnalités souhaitées	Contraintes	Exigences
- Mettre en place une solution qui permette de diminuer, voire annuler, le temps de latence observé lors de l'accès à un média intégré dans une ressource pédagogique du service de cours en ligne.	- Supporter la montée en charge provoquée par 200 utilisateurs qui consultent simultanément un média quelconque du service de cours en ligne, - Fonctionner même sur un réseau informatique à débit limité de 128 kbit/sec.	- Intégration de la solution selon un couplage faible (peu de modifications à apporter à l'existant), - Conservation des vidéos existantes. Conversion autorisée mais pas de nouvelle production à imposer. - Pas de réécriture des ressources pédagogiques pour intégrer la solution.

Tableau 5: Synthèse de l'expression du besoin

*L'expression du besoin de ce projet CNAM est formulée dans le but de réduire, voire annuler, le temps de latence imposé aux utilisateurs du service de cours en ligne avant visualisation d'une vidéo intégrée dans un ressource pédagogique.*

*La solution à concevoir et déployer doit permettre un accès rapide, voire instantané, à une vidéo et*

*offrir la capacité de se déplacer en avant ou en arrière au sein de la plage de visualisation. De plus, la solution doit s'intégrer selon un coulage faible vis à vis de l'existant et limiter ainsi les modifications.*

---

*Ce chapitre a mis en avant le fait que l'architecture actuelle de l'espace numérique de travail permet une consultation efficace des ressources pédagogiques du service de cours en ligne. Cependant, lorsque ces ressources intègrent une vidéo, l'accès à cette dernière est retardé selon un temps d'attente variable en fonction de la taille du média et de la localisation de l'utilisateur. De plus, la consultation est discontinuë et saccadée. Ces caractéristiques nuisent à l'adoption globale du service de cours en ligne par les utilisateurs.*

*L'expression du besoin à l'origine de ce mémoire CNAM a pour objectif de concevoir et réaliser une solution qui permette de s'affranchir des limitations techniques existantes et de favoriser ainsi la mise en œuvre d'une plate-forme technique compatible avec les ambitions de l'École des transmissions dans le domaine de l'enseignement à distance.*

## 5 : CONCEPTION

*Le chapitre précédent a présenté la définition du besoin. Il s'agit de permettre la consultation de manière fluide et sans temps de latence des médias audio ou vidéo du service de cours en ligne, et cela même dans un contexte où la charge est élevée. Ce chapitre présente le processus de conception que j'ai mené afin d'identifier différentes solutions qui répondent à ce besoin.*

*Dans un premier temps, une phase d'identification des éléments du portefeuille de service impactés par le projet est menée. Cette étape doit garantir la prise en compte des bons éléments durant la conception et permettre de conserver une approche orientée service compatible avec le recueil de bonnes pratiques ITIL.*

*Ensuite, je mène une étude détaillée de l'environnement de réalisation du projet et présente le concept de zones élémentaires qui se distinguent les unes des autres en raison de leurs caractéristiques techniques ou fonctionnelles.*

*Enfin, en conservant une approche orientée service, je conçois des solutions qui permettent de répondre au besoin en les spécialisant, lorsque cela est nécessaire, à chacune des zones présentées précédemment.*

### 5.1 : Identification des services impactés par le projet

*Afin de rester compatible avec le recueil de bonnes pratiques ITIL utilisé pour le projet CAN/ENT, la phase de conception doit conserver une approche orientée service. Cette contrainte garantit ainsi de pouvoir concevoir et réaliser des solutions qui s'intègrent bien dans la structure de conduite du projet et dans l'architecture existante.*

*Pour cela, cette partie reprend l'inventaire du portefeuille de services du projet CAN/ENT et identifie pour chacun de ses éléments s'il est à prendre en compte lors de la phase de conception.*

Dans sa formulation, l'expression de besoin présentée au chapitre précédent traite des problèmes de consultation de média rencontrés lors de l'exploitation du service de cours en ligne. Partant de cet état, il pourrait sembler naturel de commencer à élaborer directement des solutions à appliquer à ce service. Cependant, **par mesure de sécurité**, je choisis au préalable de la phase de conception d'énumérer les différents services du portefeuille de services du projet CAN/ENT et d'analyser, pour chacun d'entre eux, la nécessité de les prendre en compte lors de la phase de conception. La non prise en compte d'un service concerné pourrait en effet mener à déployer des solutions incomplètes ou ne répondant que partiellement à l'expression de besoin (contraintes et exigences).

Cette analyse est synthétisée dans le tableau ci-dessous et reprend pour base de départ les éléments du portefeuille de service du projet CAN/ENT présentés dans le chapitre de l'existant technique. Pour chacun d'entre eux, la justification de l'intérêt d'une prise en compte en conception est décrite.



Nom du service	Description	Prise en compte pour la conception
<b>Accès et authentification</b>	Couvre l'aspect physique, logique et la sécurisation du réseau d'enseignement.	<b>Oui.</b> Ce service concerne des servitudes utilisées par le service de cours en ligne.
Messagerie	Fonctionnalité de mail	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Emploi du temps en ligne	Permet la consultation des emplois du temps de stagiaire et de formateur	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
<b>Cours en ligne</b>	Consultation en ligne de supports de cours convertis au format numérique	<b>Oui.</b> Ce service est au cœur du besoin
Référencement des ressources SIC	Accès indexé aux ressources pédagogiques	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Ticket d'incident	Déclaration et prise en compte des incidents	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
TV en ligne	Consultation en zone d'hébergement de chaînes de TV numérique dans un navigateur.	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Forum professionnel	Forum de discussion	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Espace de stockage utilisateur	Lecture et écriture de fichier dans un espace de stockage personnel accessible par le web	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Liste de diffusion	Envoyer des mails à plusieurs destinataires avec une seule adresse	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Annuaire	Consultation des coordonnées d'un stagiaire ou d'un formateur	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Chaîne éditoriale	Publication contrôlée et versionnée de document	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes
Générateur de QCM	Contrôle de connaissances en ligne	<b>Non.</b> Ce service ne concerne pas les cours en ligne ou ses servitudes

Tableau 6: Les services à prendre en compte lors de la conception

Comme le présente le tableau d'analyse précédent, **deux services** (lignes grisées) **du portefeuille de services sont à prendre en compte pour la phase de conception.**

Le service de **cours en ligne** est sélectionné car il est au cœur de l'expression de besoin.

Le second service à intégrer traite de l'**accès et de l'authentification**. Ce service rassemble les éléments qui participent au maintien en cohérence du point de vue de l'intégrité et des performances des ressources informatiques, tant au niveau de leur acheminement que de leur protection. C'est un service de bas niveau qui englobe des fonctionnalités telles que l'authentification, le routage logiciel, le filtrage, l'optimisation des débits, la qualité de service. Globalement, tous les personnels en charge de l'administration des systèmes et des réseaux concourent à son fonctionnement. Ce service doit être pris en compte dans la phase de conception car il participe activement à l'acheminement des ressources informatiques nécessaires au bon

fonctionnement du service de cours en ligne.

L'analyse des différents éléments du portefeuille de services de l'espace numérique révèle la nécessité de prendre en compte deux services durant la phase de conception :

- Le service de cours en ligne, partie intégrante de l'expression de besoin,
- Le service d'accès et authentification qui joue un rôle de premier ordre vis à vis des ressources informatiques nécessaires au bon fonctionnement du service de cours en ligne.

Ces deux services sont à la base de la stratégie générale de conception présentée ci-dessous.

## 5.2 : Stratégie générale de conception

L'étude de l'existant technique a présenté le fait que l'architecture générale du réseau d'enseignement connecté à l'Internet a des caractéristiques variables selon la localisation de ses éléments. De ce fait, une solution unique et globale présentera un comportement différent selon son lieu d'utilisation. Pour cette raison, j'ai choisi de prendre en compte les zones élémentaires de l'architecture technique du projet et d'identifier les liaisons de réseau qui les relient les unes aux autres. J'ai alors mis en place une stratégie de conception qui permette de traiter chacun de ces éléments.

L'étude de l'existant technique a déjà présenté l'architecture générale du réseau d'enseignement Internet de l'école. Elle se compose de **cinq zones élémentaires** correspondants à la zone WAN Internet, la zone d'hébergement, la zone des plates-formes d'instruction et des stations de consultation, la salle des serveurs et la zone démilitarisée (DMZ), comme le présente l'illustration ci-dessous.

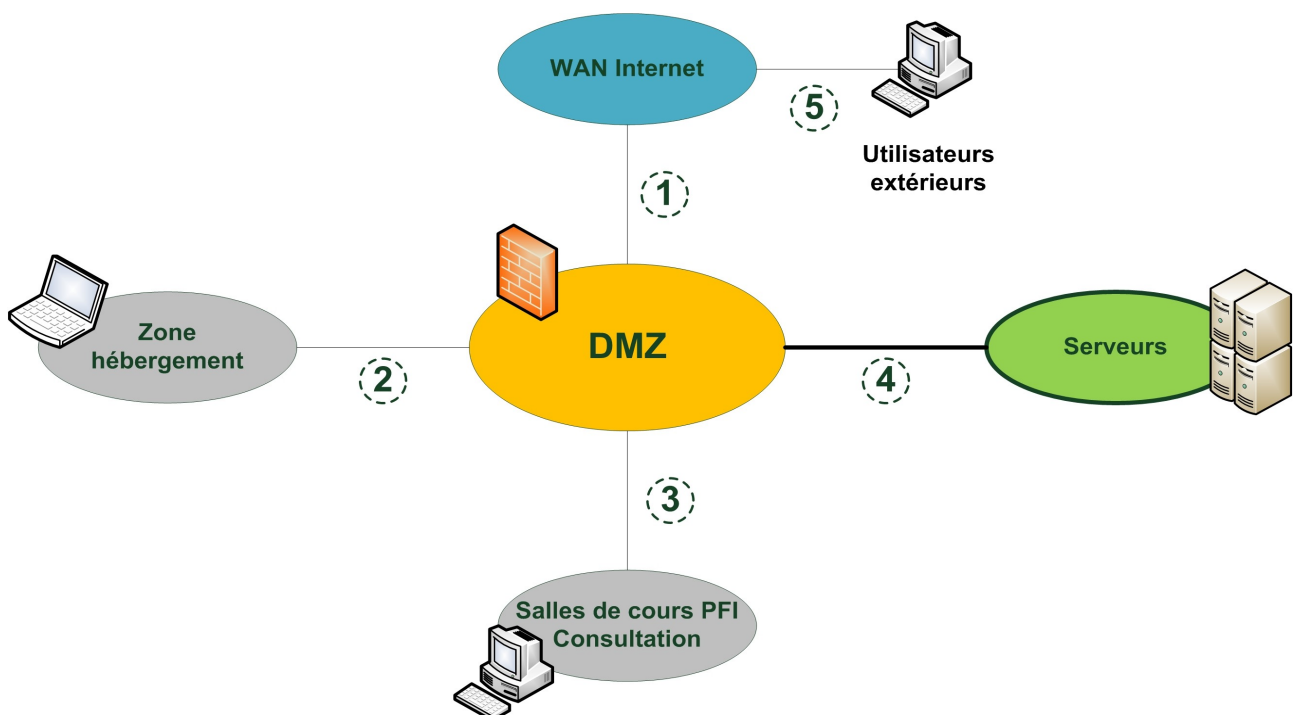


Illustration 16: Découpage en zones élémentaires du réseau d'enseignement connecté à l'Internet

Toutes ces zones présentent des caractéristiques techniques qui leur sont propres et sont hétérogènes. Par exemple, certaines d'entre elles sont protégées par des règles de firewall personnalisées. Les portions de réseau qui les relient les unes aux autres, **numérotées de 1 à 5** sur

le schéma précédent, présentent des caractéristiques de routage ou de débit différentes. C'est pourquoi j'ai choisi d'appréhender chacune de ces zones ou liaisons de manière individuelle au cours de ma conception plutôt que de tenter la réalisation d'une solution unique et globale qui nivellerait ses capacités par le bas. Cette contrainte supplémentaire augmente considérablement la charge de travail de conception et de réalisation puisqu'elle multiplie les actions à mener. Cette organisation permet cependant de réaliser des solutions au comportement uniforme en tout point de l'architecture.

La **stratégie générale** retenue pour mener la phase de conception de mon projet consiste donc à **analyser les éléments selon deux niveaux d'abstraction** :

**Le premier niveau d'abstraction** s'attache à **étudier de manière indépendante les services concernés par le projet**. Il s'agit du service de cours en ligne et du service d'accès et d'authentification présentés en première partie de ce chapitre. Ainsi, je mène deux phases de conception, chacune rattachée à l'un des services concernés. Ce niveau d'abstraction permet de conserver une approche orientée service et donc de rester compatible avec le recueil de bonnes pratiques ITIL<sup>10</sup>.

**Le second niveau d'abstraction** appliqué consiste à **prendre en compte les zones élémentaires de l'architecture ainsi que leurs liaisons** (celle numérotées de 1 à 5 dans le schéma précédent) pour chaque phase de conception. Ce niveau d'abstraction supplémentaire permet cette fois de prendre en compte les caractéristiques propres à chacune des zones et liaisons lors de la conception des solutions rattachée à chaque service..

Les prochaines parties de ce chapitre présentent le déroulement de cette stratégie en commençant par le service d'accès et d'authentification et en terminant par le service de cours en ligne, plus dépendant du premier. Pour chacun des services, le second niveau d'abstraction est appliqué et les éléments de l'architecture générale du réseau d'enseignement (zones ou liaisons) qui doivent être pris en compte sont traités.

Enfin, la conception des solutions respecte l'approche conseillée par le recueil de bonnes pratiques ITIL. Elle favorise de fait la reprise potentielle de mes travaux par un autre membre du projet CAN, déjà initié à cette technique.

ITIL préconise l'exécution de nombreux sous-processus lors de la phase de conception d'une solution. Cependant, tous ces sous-processus ne sont pas systématiquement applicables à chaque projet. Le choix est laissé au concepteur en fonction de l'environnement et du cadre d'exécution de la démarche. Dans l'ensemble, les sous-processus que j'ai exécutés dans le cadre de ce projet CNAM m'ont permis de prendre en compte, lorsque cela était réalisable, les aspects suivants lors de la conception de mes solutions :

- Gestion de la **capacité** : étude de l'aptitude à gérer les exigences futures, telle la résistance à la montée en charge ou l'évolution du besoin en ressources,
- Gestion de la **disponibilité** : étude de la capacité à maintenir et assurer le service à rendre,
- Gestion de la **continuité** : étude de la capacité à proposer des solutions alternatives en cas de dysfonctionnement,
- Gestion de la **sécurité** : étude de la capacité à se protéger des actions mal intentionnées,
- Gestion des **sous-traitants** : étude du besoin et des formalités de sous-traitance,
- Gestion de la **configuration** : étude des paramètres et des réglages à appliquer à la solution,

---

10 Une présentation du recueil de bonnes pratiques ITIL est fournie en annexe II

- Gestion de la **connaissance** : étude et prise en compte de la formation nécessaire à l'utilisation de la solution,
- Gestion de la **mise en production** : étude amont de la transition vers la mise en œuvre opérationnelle.

La sélection de ces sous-processus a été validée par M. Martineau, Officier en Management du Système d'Information. En cohérence avec cet accord, le formalisme des conceptions présentées plus bas dans ce chapitre a volontairement écarté une organisation présentant la gestion de ces sous-processus selon un mode séquentiel organisé en paragraphes distincts. Ce choix s'explique par le fait que selon les situations, la prise en compte d'un sous-processus est parfois simple ou réduite et ne justifie pas systématiquement une déclaration formelle et explicite.

*La stratégie générale de conception mise en œuvre dans mon projet repose sur deux niveaux d'abstraction. Le premier niveau prend en compte les services du portefeuille de services impactés par le projet. Le second niveau prend en compte les zones élémentaires de l'architecture technique générale et les liaisons qui les relient ensemble. Enfin, chaque processus de conception est mené dans le respect des bonnes pratiques ITIL v3 et dans la juste utilisation de son formalisme.*

## 5.3 : Conception associée au service d'accès/authentification

*Cette partie présente les différentes conceptions que j'ai menées dans le but d'apporter au service d'accès et d'authentification des solutions capables d'améliorer ses caractéristiques et ses aptitudes à répondre à l'expression de besoin du projet.*

*Dans un premier temps, les zones élémentaires de l'architecture générale et les éléments de liaison à prendre en compte sont recensés afin de définir le second niveau d'abstraction de la stratégie générale de conception. Ensuite, pour chacun des éléments identifiés, une solution est conçue et proposée.*

### 5.3.a) Les zones élémentaires et les liaisons à prendre en compte

L'identification des zones élémentaires et des liaisons à prendre en compte pour la phase de conception associée au service d'accès et d'authentification est simple. En effet, nous avons déjà vu que ce service participe au maintien en cohérence des ressources informatiques, tant au niveau de leur acheminement que de leur protection. Les éléments qui doivent faire l'objet d'une conception personnalisée pour ce service correspondent donc à **toutes les liaisons** sur lesquelles il est possible d'intervenir à l'ETRS (voir l'illustration n°16). Les zones élémentaires ne font pas l'objet d'une attention particulière puisqu'elles sont déjà prises en compte à chaque extrémité des liaisons et conditionnent de fait la nature même des liaisons.

En référence au schéma d'architecture générale présenté dans la partie précédente, les liaisons identifiées à prendre en compte sont :

- Liaison n°1 : Entre WAN Internet et DMZ,
- Liaison n°2 : Entre zone d'hébergement et DMZ,
- Liaison n°3 : Entre PFI/Consultation et DMZ,
- Liaison n°4 : Entre les serveurs et la DMZ

Nous verrons plus bas dans ce chapitre pourquoi la liaison n°5, située entre les utilisateurs extérieurs et le WAN Internet, ne peut pas être traitée dans le cadre de ce projet.

### 5.3.b) Liaison N°1 : WAN Internet et DMZ

#### - Étude amont

La connexion entre le WAN Internet et la DMZ est une liaison majeure qui réalise le lien entre le réseau Internet mondial et l'architecture technique de l'école reliée à l'Internet. Cette liaison est assurée par un abonnement avec un tiers fournisseur d'accès. Bien que l'école ait souscrit un contrat de service lui assurant une intervention dans les 24 heures en cas de panne, elle ne dispose pas de réel moyen de contrôle sur cette source de données.

Cette liaison est positionnée en coupure de réseau entre le réseau Internet et la partie intérieure de l'école. Son indisponibilité provoquera donc l'indisponibilité de l'ensemble des services du portefeuille de services de l'ENT pour tous les utilisateurs qui exploitent le mode de partage de la connaissance en enseignement à distance depuis l'extérieur de l'école. Par conséquent, cette liaison qui existe déjà joue un rôle majeur dans la disponibilité du service de cours en ligne. J'en conclus donc qu'il est nécessaire de concevoir une solution qui permette de renforcer sa disponibilité.

Pour faire face à une interruption de service au niveau du WAN Internet, il me paraît donc nécessaire de mettre en place un système de redondance de réseau. Ainsi, en cas de panne, les conséquences d'une défaillance seront masquées ou réduites. Cette redondance concerne ici la source d'approvisionnement en réseau Internet. Il ne s'agit pas de dupliquer à l'identique le matériel qui compose la liaison, tels les câbles ou les matériels actifs.

Après analyse des solutions possibles (pour laquelle je ne fournis ici que la synthèse par esprit de concision), il apparaît que **deux solutions** permettent la mise en place d'une redondance de réseaux.

**La première** consiste à **souscrire un abonnement auprès de deux fournisseurs d'accès différents** et de connecter les sources à un élément actif spécialisé permettant de gérer les deux lignes.

La configuration de base de ce type d'équipement met en place un système de répartition de charge de type « load balancing<sup>11</sup> ». Lorsqu'un utilisateur initie une nouvelle connexion, l'équipement de balance de charge lui affecte une seule ligne pour toute la durée de la transaction. Si un autre utilisateur initie une nouvelle connexion, l'équipement lui affecte alors la ligne qui n'a pas été sélectionnée précédemment. Ainsi, le « load balancing » ne permet pas d'additionner le débit des deux lignes mais répartit efficacement la charge sur chacune d'entre elles.

Si les deux lignes sont à niveau de débit égal, les utilisateurs n'ont jamais conscience du dispositif mis en jeu et lorsqu'une ligne est indisponible, l'équipement permet un mode dégradé en exploitant uniquement la seconde jusqu'à ce que la situation soit rétablie.

Dans un mode de configuration plus avancé, il est également possible d'affecter un ordre de priorité aux différentes lignes employées et de privilégier l'utilisation d'une ligne par rapport à une autre selon le protocole utilisé ou la destination. Il peut alors être intéressant de désigner une ligne principale et de souscrire des options de débit plus important ou de dépannage plus rapide. Cette ligne peut ensuite être employée pour initier les transactions indispensables vers le serveur d'authentification ou celles plus consommatrices de bande passante vers les ressources multimédias ou, enfin, celles plus critiques à destination des salles de cours. La ligne offrant le meilleur débit ascendant du LAN vers le WAN peut être utilisée en priorité pour diffuser les contenus à destination des utilisateurs situés à l'extérieur de l'école. A l'inverse, les stations des cadres peuvent exploiter une seconde ligne moins performante.

Suivant les options de dépannage souscrites, la logique veut que les périodes d'indisponibilité de la ligne principale soient peu fréquentes. De ce fait, **la qualité de service d'une telle configuration est excellente** et permet néanmoins un fonctionnement en mode dégradé lorsqu'une seule ligne sur les deux est disponible.

En revanche, l'inconvénient d'une redondance de réseaux basée sur un double abonnement réside dans **l'absence total de contrôle du chemin emprunté par les données** pour arriver jusqu'au boîtier de fusion des lignes. Ainsi, deux abonnements différents souscrits auprès de tiers concurrents pourront néanmoins exploiter le même répartiteur de niveau WAN. Des travaux d'infrastructure dans le quartier nécessitant l'arrêt de ce répartiteur provoqueront alors l'interruption des deux réseaux. Il s'agit donc d'une redondance logique et non physique des réseaux. Ces aspects peuvent être considérés comme une vulnérabilité.

---

<sup>11</sup> Le « load balancing » indique un système capable d'assurer une balance de charge en adressant de manière séquentielle les éléments qui lui sont rattachés. Le « load balancing » est très utilisé pour les sites web qui répartissent leur charge sur plusieurs serveurs.

Pour pallier à cet inconvénient, il existe une **deuxième solution** permettant la redondance de réseaux. Elle consiste à souscrire **un abonnement spécifique** avec un seul fournisseur d'accès auprès duquel une option de **redondance de répartiteur avec garantie de chemin multiple au niveau de l'architecture WAN** est ajoutée. Le coût mensuel moyen observé pour cette prestation de haute disponibilité est généralement de l'ordre de 500€ mais dans le cas d'une redondance de répartiteurs, l'indisponibilité d'un équipement de niveau WAN est transparente car les données peuvent toujours emprunter un autre chemin disponible au sein de l'infrastructure.

En aval de la solution retenue pour améliorer la disponibilité du réseau, des équipements adaptés à l'optimisation d'un type de flux particulier peuvent, là encore, être ajoutés. Par exemple; il existe des boîtiers électroniques qui permettent de mettre en œuvre une fonction de cache sur les flux HTTP. Ainsi, les ressources associées aux requêtes web les plus fréquentes sont stockées en mémoire dans l'équipement et sont restituées aux utilisateurs sans générer de nouvelle connexion réseau. Les flux HTTPS peuvent également être pris en charge à condition d'importer les certificats utilisés pour chiffrer et déchiffrer les communications. Le prix moyen observé pour ce type d'équipement se situe autour de 5000€.

Dans la même gamme de prix, il existe des boîtiers spécialisés dans la diffusion de flux multimédias qui conservent en cache des trames de réseau complètes générées une seule fois par un serveur situé en amont. Ces trames sont alors redistribuées en l'état par l'équipement qui n'a plus qu'à modifier l'adresse du destinataire.

Enfin, l'amélioration de la qualité du service d'accès/authentification peut être envisagée en mettant en œuvre le protocole IP V6 sur le réseau. Ce protocole intègre nativement des fonctions avancées de qualité de service lui permettant, par exemple, d'accélérer les processus de routage grâce à des champs dédiés ajoutés à l'entête des trames réseau. La sécurité est également améliorée avec la prise en compte par défaut de l'« Internet Protocol Security » (IPSec) qui permet de chiffrer et déchiffrer les communications dès la troisième couche du modèle OSI (couche réseau).

### **- La solution retenue**

Sur la base des éléments qui viennent d'être présentés, la solution que je retiens pour améliorer la liaison entre le WAN internet et la DMZ met en œuvre la **solution basée sur le double abonnement et le matériel actif spécialisé dans la répartition de charge**.

En effet, cette solution offre une **plus grande souplesse de configuration** que celle mettant en jeu une redondance de répartiteurs. De plus, la possibilité de pouvoir affecter une ligne plutôt qu'une autre à une zone précise permet de **mettre en place une gestion de qualité de service fine** en privilégiant les flux à destination du cœur de métier (salles de cours et plates-formes d'instruction), comme le présente le schéma n°17.

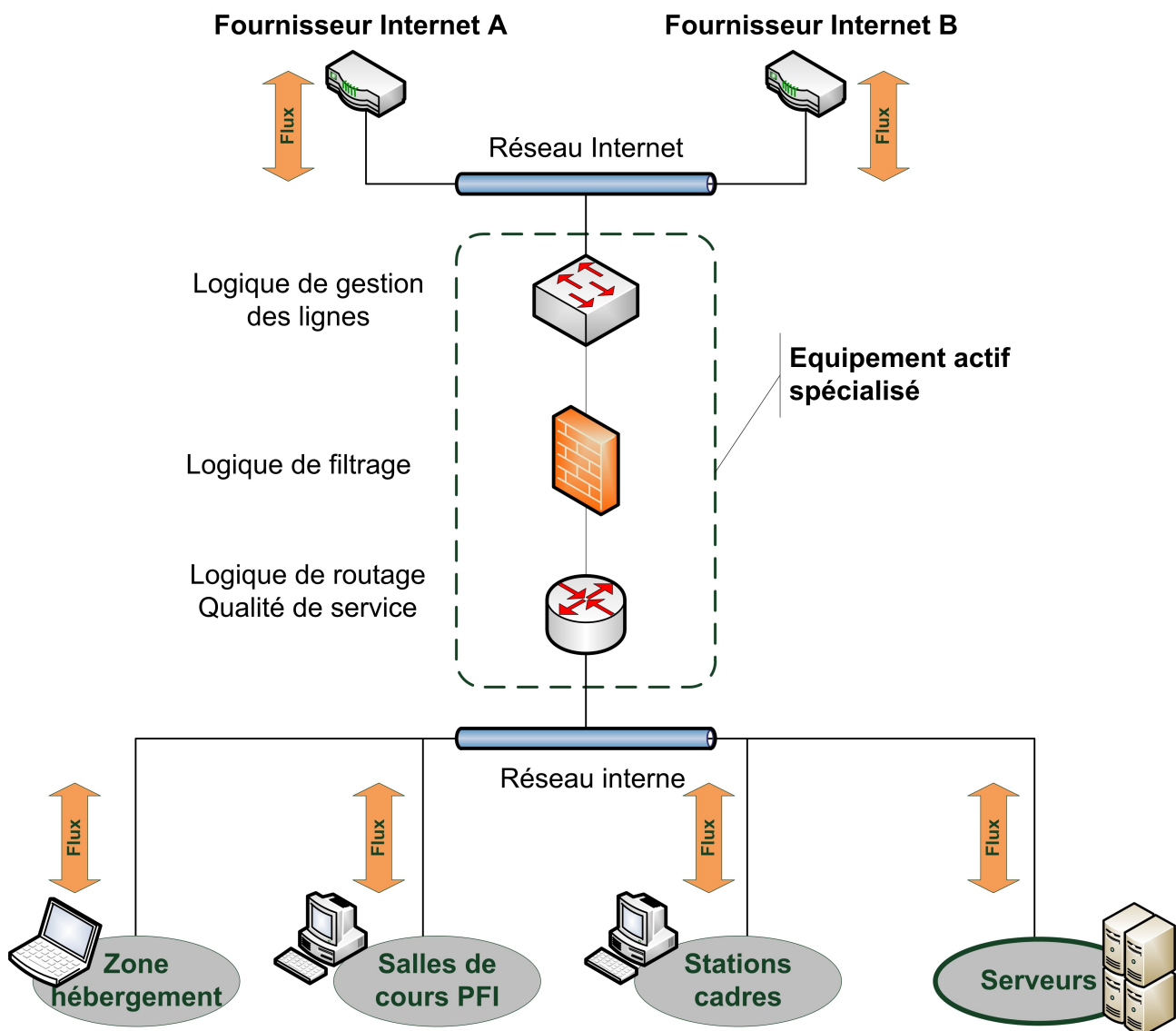


Illustration 17: Schéma de principe du double abonnement internet

Le risque de subir une interruption de service prolongée d'un concentrateur semble limité de nos jours car la popularité du réseau Internet impose une grande réactivité d'intervention aux techniciens en charge des matériels. Il n'existe pas d'étude comparative présentant avec suffisamment de précision le pourcentage de disponibilité de chacun des fournisseurs d'accès à l'Internet. Cependant, force est de constater que la disponibilité globale des lignes est très satisfaisante. De ce fait, et même si le risque d'indisponibilité d'un matériel de niveau WAN existe, je ne retiens pas ce critère pour déterminer le choix de ma solution.

L'équipement nécessaire au déploiement de la solution est disponible sur étagère chez les fournisseurs de matériel réseau. Par exemple, la série ASA 5500 (Adaptive Security Appliances) de la société CISCO propose une gamme de matériels électroniques permettant de mettre en œuvre la répartition de charge entre réseaux. Suivant les options retenues, ces équipements peuvent intégrer un logiciel de gestion de qualité de service et un firewall. Pour une telle configuration, le prix de vente constaté évolue alors autour de 5 000€. Mon choix pour ce matériel est renforcé par le fait que l'école en a actuellement un exemplaire à sa disposition et que ce dernier est disponible à l'utilisation.



**Le personnel exploitant l'équipement doit disposer de connaissances en administration système** lui permettant de maîtriser la notion de réseau logique afin de bien identifier les zones à gérer et régler correctement le firewall. La prise en main de l'interface d'administration du système doit également être totale. Pour cela, **une assistance à l'utilisation peut être souscrite auprès du fournisseur de l'élément actif** durant la première année de mise en service.

En raison de la position très en amont de l'équipement à installer vis à vis du réseau de l'école, **le déploiement de la solution est une étape critique** qui met en jeu la disponibilité du système d'information de la formation dans sa totalité. A ce titre, **la capacité à revenir rapidement et facilement à l'ancienne configuration doit être maintenue** tant que la solution n'est pas pleinement validée afin de palier aux éventuels dysfonctionnements qui n'auraient pas été anticipés durant les phases de test.

**L'impact sur le reste de l'architecture existante est nul.** En effet, la mise en production de la solution ne nécessite pas de corriger la configuration des serveurs ou des stations clientes en place. En revanche, **l'utilisation de l' « IP V6 » n'est pas retenue** car bien que son exploitation apporte des améliorations indéniables, les modifications à apporter sur l'architecture pour la rendre pleinement compatible avec ce protocole nécessite d'installer des correctifs logiciels (pilotes de carte réseau, configuration logique des clients, etc.) sur l'ensemble des machines du réseau et de revoir la configuration des matériels actifs.

Enfin, pour des **raisons de sécurité relatives à la protection et à l'intégrité des données** telles qu'elles sont explicitées par la PSIAT, le matériel doit être installé dans une **salle technique sécurisée** équipée de portes blindées et de fenêtres à barreaux qui limitent les possibilités d'intrusion physique. Actuellement, seule la salle dédiée à l'hébergement des serveurs propose cette configuration à l'école.

### **5.3.c) Liaison n°2 : Zone hébergement et DMZ**

#### **- Étude amont**

La liaison entre la zone d'hébergement et la DMZ permet d'acheminer le réseau Internet jusque dans la chambre des stagiaires résidents. L'école ne fournit pas les postes informatiques permettant de réaliser la connexion. C'est le matériel personnel des stagiaires qui est utilisé. A ce titre, la configuration des machines n'est pas maîtrisée comme elle peut l'être avec les postes de bureau de l'école où seul les administrateurs ont pu installer le système d'exploitation et les logiciels disponibles. Pour cette raison, la zone d'hébergement constitue **une zone sensible en termes de sécurité informatique** dans le sens où **le potentiel de nuisance est plus important** que dans les zones où la configuration des postes est maîtrisée.

Pour pallier à cet inconvénient, l'accès à la DMZ depuis la zone hébergement est soumis à une authentification auprès d'un portail captif qui interdit tout trafic aux stagiaires tant que ceux-ci ne se sont pas explicitement identifiés. La solution employée met également en œuvre un firewall qui permet de définir des règles de filtrage pour protéger les accès. Le portail captif actuellement utilisé est une solution Microsoft nommée « Captivate » qui vient se greffer sur le firewall d'entreprise du même fournisseur nommé « ISA Server ».

Cette configuration présente actuellement **trois inconvénients majeurs** :

En premier lieu, l'annuaire de référence des comptes utilisateurs du portail captif est alimenté par le

serveur Active Directory du réseau interne de l'école. Au demeurant, cette configuration ne présente pas de problème. Cependant, ce n'est pas cet annuaire qui est utilisé par le système d'authentification centralisée de l'espace numérique de travail. Ce dernier doit en effet nécessairement exploiter un annuaire de type LDAP afin de permettre l'exploitation de ses fonctionnalités avancées. **Cette organisation impose donc un double système d'authentification.** Ainsi, un stagiaire souhaitant accéder à l'ENT depuis sa chambre doit d'abord s'authentifier une première fois auprès du portail captif pour accéder à l'Internet puis une seconde fois auprès du système d'authentification centralisée s'il veut, par exemple, consulter ses mails, son emploi du temps ou accéder au service de cours en ligne. **La redondance d'identifications nuit à l'accès aux services de l'espace numérique de travail depuis la zone d'hébergement** car elle contraint l'utilisateur à saisir deux noms de connexion et mots de passe avant de pouvoir y accéder. Par extension, **l'accès au service de cours en ligne est freiné par cet état de fait.**

Le second inconvénient de la solution courante réside dans ses **faibles capacités à tracer et imputer les actions des utilisateurs.** Par exemple, le système ne permet pas de retrouver l'identité d'une personne en fonction du jour, de l'heure de connexion et de la destination de sa navigation. De ce fait, l'école ne peut pas identifier précisément l'auteur d'un accès vers un site web à caractère interdit ou illicite. Cette situation ne répond pas aux exigences de la politique de sécurité de l'armée de Terre. De plus, l'école court le risque de subir une coupure générale de sa ligne Internet imposée par décision de justice en cas d'accès à un site interdit, faute de pouvoir identifier clairement le responsable. **L'éventualité d'une coupure de la ligne Internet de l'école fait courir un risque d'indisponibilité pour tous les services de l'espace numérique de travail.** Dans le cadre de ce projet, c'est donc la disponibilité du service de cours en ligne qui est menacée.

Enfin, des **études menées par le cours de sécurité informatique de l'école** ont révélé des **insuffisances en termes de protection et d'efficacité de la solution actuelle.** Une personne formée aux techniques d'usurpation d'identité par modification des trames de données qui sortent de la carte réseau de la machine pourra en effet profiter d'une connexion autorisée sans passer par une phase d'authentification. Cette compétence est classique pour un pirate informatique. Ce constat n'est pas acceptable, d'autant plus que les stagiaires du cours de sécurité informatique apprennent eux-même ces techniques afin de mieux comprendre les protections à mettre en place pour s'en protéger. Ainsi, **les possibilités actuelles de protection mises en œuvre en zone d'hébergement ne sont pas satisfaisantes vis à vis des services de l'espace numérique de travail.** Cette fois encore, le service de cours en ligne est donc impacté par le problème.

### **- La solution retenue**

A partir des analyses et critiques formulées précédemment, je retiens la **nécessité de mettre en place une nouvelle solution de portail captif** pour protéger la liaison entre la zone d'hébergement et la DMZ.

Les fonctionnalités à assurer doivent permettre :

- De journaliser et d'archiver précisément les actions des utilisateurs afin de permettre l'imputabilité de leurs actions,
- De protéger efficacement la zone située derrière le portail captif (école et réseau Internet) et de rendre inopérantes les tentatives d'usurpation d'identité,
- D'exploiter l'annuaire des utilisateurs déjà employé par le système d'authentification centralisée de l'espace numérique de travail pour permettre, **à terme**, de fusionner et supprimer la contrainte de double authentification.

Après étude des différentes offres en la matière (étude dont seule la synthèse est présentée ici), il apparaît qu'il existe une offre pléthorique de solutions de portails captifs performants, capables d'exploiter une source de données connectée à un annuaire LDAP et à même de déjouer les tentatives de contournement des dispositifs de sécurité. Leur technologie est identique aux Hot-Spot WIFI installés dans les lieux publics tels les gares, les aéroports ou les hôtels. Les plus connus se nomment PepperSpot, ChilliSpot, Zeroshell, Pfsense ou Alcasar.

Parmi la liste des portails captifs recensés, le produit Alcasar (<http://www.alcasar.info>) se dégage naturellement à l'ETRS car **son équipe de développement est notamment animée par la majeure partie des acteurs du cours SSI de l'école**. De plus, ce produit a déjà été déployé sur de nombreux sites institutionnels membres de la communauté ADULLACT<sup>12</sup> (Association des Développeurs et des Utilisateurs de Logiciels Libres pour l'Administration et les Collectivités Territoriales) et fait état d'un retour d'expérience très positif.

Cette solution présente l'avantage de constituer **une solution de sécurité qui regroupe les fonctionnalités de portail captif et de firewall intégrées sur une seule machine**. L'équipement est positionné en coupure de réseau et se comporte en passerelle sécurisée que l'on ne peut traverser qu'après avoir réussie la phase d'authentification imposée. Le déploiement de la solution sur la machine est assuré par **un script d'installation qui prend en charge la totalité du processus**.

**Le lien entre les utilisateurs et le portail captif** peut s'effectuer de manière classique avec une liaison Ethernet mais également au travers d'un point d'accès WIFI qui permet ainsi l'utilisation des périphériques sans fil, comme le présente le schéma ci-dessous.

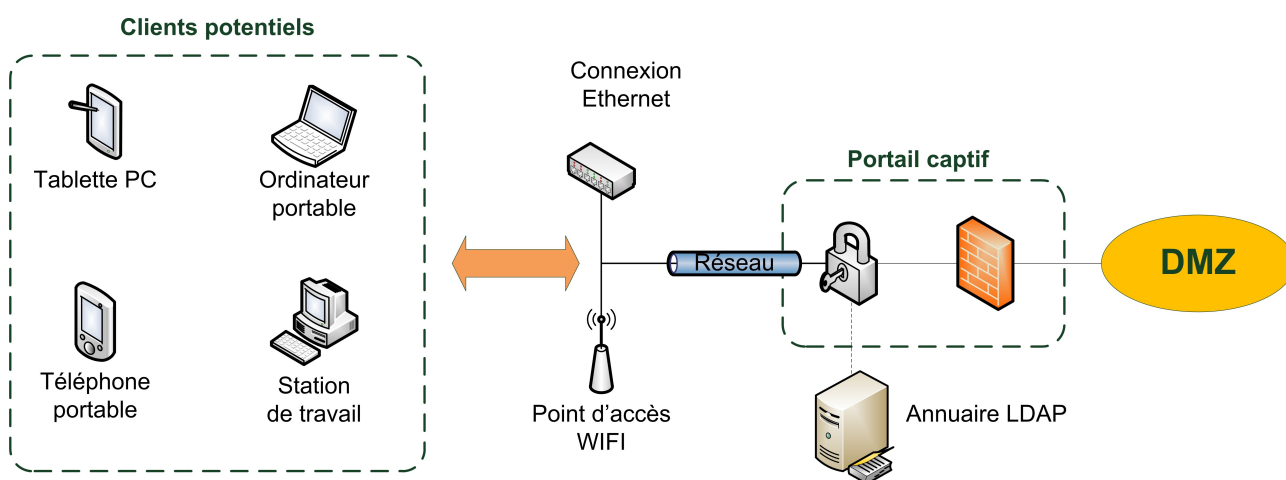


Illustration 18: Installation d'un portail captif en coupure de réseau

La possibilité d'accéder au réseau de l'école par une liaison WIFI depuis la zone d'hébergement est une possibilité intéressante pour les stagiaires. Ils pourraient alors utiliser leurs équipements mobiles pour accéder à l'ENT.

Puisqu'il se situe en amont du portail captif, le point d'accès WIFI peut être configuré en accès public libre et non protégé. Seul le chiffrement des communications est **impératif** afin de masquer le nom de connexion et le mot de passe transmis au portail captif lors de l'authentification.

12 La communauté ADULLACT s'est donnée pour objectifs de soutenir et coordonner l'action des collectivités territoriales, des administrations publiques et des centres hospitaliers dans le but de promouvoir, développer, mutualiser et maintenir un patrimoine commun de logiciels libres utiles aux missions de service public.

L'installation du WIFI en zone d'hébergement n'est pas prévue pour le moment mais j'ai pu réaliser une configuration identique au sein de l'école durant les journées de rencontre du numérique et elle a donné d'excellents résultats<sup>13</sup>.

**L'insertion en coupure de réseau du portail captif ne permet pas le fonctionnement en mode dégradé.** Soit l'équipement est en mode nominal et l'accès au réseau est possible, soit il est hors service et la fonctionnalité est interrompue. A ce titre, **une politique de sauvegarde journalière des données doit être mise en place** afin d'être en mesure de restaurer tout ou partie du système en cas de nécessité.

Pour pallier à un dysfonctionnement matériel, **un second ordinateur et des cartes réseaux identiques à l'équipement en production doivent être conservés et maintenus en réserve.** Le montage **d'un second disque dur configuré en miroir du premier** est réalisé dans la configuration principale. Ainsi, les administrateurs disposeront en permanence d'un équipement de rechange complet et d'un disque dur opérationnel synchronisé avec l'existant.

L'interface d'administration du portail Alcasar est conçue pour masquer la complexité des actions sous-jacentes réalisées sur le système. De ce fait, **la formation des administrateurs en charge de l'équipement est réduite à l'apprentissage du processus d'enregistrement des utilisateurs** car les connaissances inhérentes à leur fonction sont suffisantes pour appréhender le fonctionnement global du produit. De plus, la présence dans les locaux des concepteurs du portail garantit une **assistance à l'utilisation de qualité** sans nécessiter la mise en place d'un contrat de service facturé.

Enfin, **la transition à prévoir lors de la mise en production de la solution est réduite.** En effet, à la mise en service, les utilisateurs constateront simplement que c'est une nouvelle page web d'authentification qui s'affiche dans leur navigateur lorsqu'ils accèdent au réseau. La seule particularité à prendre en compte réside dans le fait que le portail captif exploitera dorénavant l'annuaire LDAP de l'espace numérique de travail et non l'annuaire Active Directory de la configuration précédente. De ce fait, **ce ne sont plus les mêmes noms de connexion et mots de passe qui devront être utilisés.** Cette information **doit être rendue visible** en modifiant le code source de la page web d'authentification du portail afin d'y faire apparaître un encart de texte libre dédié à cet effet.

### **5.3.d) Liaison n°3 : PFI/Consultation et DMZ**

#### **- Étude amont**

La liaison entre la DMZ et le regroupement formé par les plates-formes d'instruction et les stations de consultation permet d'acheminer le réseau Internet à l'intérieur de l'école (exception faite de la zone d'hébergement traitée par la liaison précédente). De ce fait, **cette liaison participe à la disponibilité générale du système d'information de la formation à l'intérieur de l'école.**

Le transfert des informations entre les deux points de la liaison est soumis à un **filtrage logiciel réalisé par un firewall.** Une **fonction de routage** est également mise en œuvre pour assurer la communication entre les éléments car ces derniers n'ont pas la même configuration logique (adresse IP, masque de sous-réseau, adresse de passerelle) à chaque point de la liaison.

Comme je l'ai présenté dans l'étude de l'existant pédagogique, je suis responsable de la cellule en

---

<sup>13</sup> Les rencontres du numérique ont eu lieu à l'ETRS au mois de mai 2010 et ont permis de réunir différents acteurs impliqués dans le monde de l'enseignement numérique.

charge de l'architecture technique des systèmes d'information. A ce titre, j'ai pu disposer des droits d'administration nécessaires pour procéder à l'installation du système de supervision NAGIOS (<http://www.nagios.org>) sur les serveurs et les équipements de l'architecture. Ce système permet d'effectuer des sondages et des tests sur ses clients et notamment des mesures de débit régulières sur les cartes réseau d'un équipement.

Actuellement, les fonctions de filtrage et de routage de la liaison étudiée ici sont assurées par un seul ordinateur équipé de deux cartes réseau. J'ai utilisé les mesures de débits réalisées par le système NAGIOS pour analyser le trafic réseau géré par cet ordinateur.

En premier lieu, et comme le présente l'illustration ci-dessous, on distingue sur le graphe de débit de la **carte externe située du côté de la DMZ des volumes en entrée (en rouge) plus importants que ceux en sortie (en vert)**. Ce résultat indique que l'utilisation actuelle de la ligne est principalement **orientée vers la consultation du réseau Internet et non vers la distribution de services vers l'extérieur**.

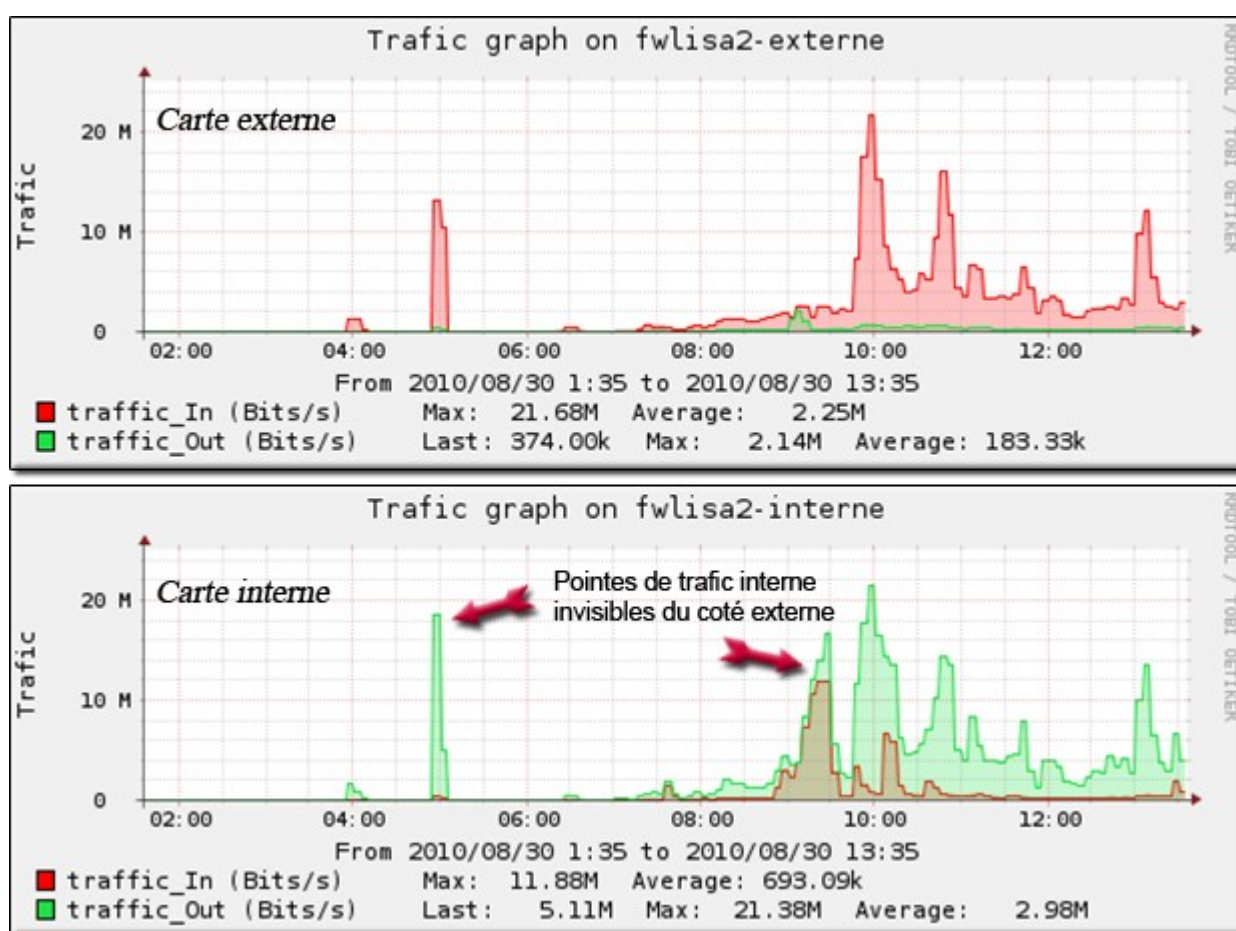


Illustration 19: Mesures de débit sur la carte réseau interne et externe de l'équipement

Du côté de la **carte interne**, l'allure du **trafic en sortie (en vert)** ressemble sensiblement à celle du **trafic en entrée de la carte externe (en rouge)** et confirme que l'équipement a un comportement « suiveur » qui achemine des données depuis l'extérieur. Il existe cependant des périodes où le trafic en entrée de la carte interne provoque des pointes de volume en sortie sans que cela soit visible sur la carte externe. Ces créneaux, repérés par des flèches rouges sur l'illustration n°19 indiquent **des phases de routage interne denses** et correspondent à des **périodes de trafic important qui n'ont lieu que sur le réseau interne de l'école** sans générer de trafic au delà de la

carte externe.

Ces phases de routage denses provoquent un débit en pointe de 20 Mbits/sec sur le réseau interne de l'école. Les équipements actifs qui forment ce réseau sont conçus pour supporter un débit maximum de 100 Mbits/sec. Il reste donc une bande passante théorique de 80 Mbits/sec disponible. Cette valeur est faible compte tenu de la mise en œuvre prochaine d'une solution de diffusion de flux multimédias associée au service de cours en ligne. Bien que je ne sois pas encore capable de mesurer pleinement l'impact de la mise en place de cette solution sur le réseau, je dois d'ores et déjà **prévoir dans mon architecture l'éventualité d'une saturation de la bande passante en raison d'un effort de routage trop important**. En effet, il ne peut être question de devoir stopper le service de cours en ligne à l'intérieur de l'école parce que l'équipement en charge du routage interne est saturé.

D'autre part, l'infrastructure mise en œuvre pour acheminer le réseau Internet jusqu'aux plates-formes d'instruction et les stations de consultation ne permet pas une isolation des deux lignes. Les équipements actifs installés dans les différents bâtiments sont utilisés conjointement quel que soit la destination. Cette configuration nuit à la qualité du service d'accès/authentification car elle **ne permet pas d'isoler les flux entre les différents réseaux et diminue ainsi leur capacité d'exploitation respective**. Par exemple, un virus situé sur le réseau des stations de consultation pourra contaminer le réseau des plates-formes d'instruction puisque les lignes ne sont pas isolées.

Enfin, et toujours en utilisant le système NAGIOS, des mesures de charge moyenne réalisées sur les processeurs de l'équipement et présentées dans l'illustration ci-dessous font observer des pointes d'activité qui ne dépassent pas vingt pour-cents du temps processeur. Ces mesures indiquent que **la fonction de filtrage sollicite faiblement l'équipement analysé**.

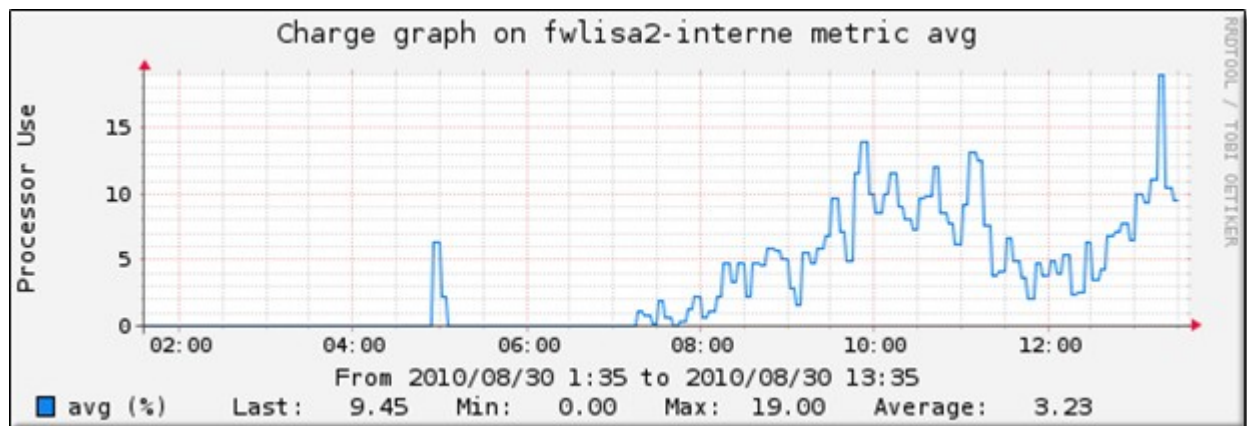


Illustration 20: Mesure d'activité moyenne des processeurs de l'équipement

Cette observation est confortée par les mesures de l'illustration n° 19 qui indiquent qu'il n'existe pas de période où le trafic en entrée de la carte interne s'inscrit dans un créneau où son trafic en sortie soit inférieur au trafic en entrée de la carte externe. Ces mesures confirment bien que **la fonction de filtrage a un impact faible sur le débit général observé sur le réseau** et que peu de paquets de données sont bloqués par le firewall.

En synthèse des différents éléments présentés précédemment, nous pouvons donc retenir les éléments suivants :

- La fonction de filtrage est faiblement sollicitée au sein de la liaison et a peu d'impact sur le trafic général,

- L'architecture actuelle provoque déjà des pics de volume ponctuels liés à du routage interne. Ce routage consommera peut être toute la bande passante disponible lorsque la solution de diffusion de flux multimédias associée au service de cours en ligne sera opérationnelle,
- Il n'existe pas de distinction entre le réseau qui dessert les stations de consultation et celui qui dessert les plates-formes d'instruction.

En regard de ces éléments, je retiens donc la nécessité de mettre en place une solution qui permettent de **gérer une forte charge de routage interne sans risque de saturation**. Cette solution doit d'autre part permettre d'**isoler les lignes qui adressent le réseau des plates-formes d'instruction et celui des stations de consultation**. Enfin, il est nécessaire de **maintenir une fonction de filtrage** tout en sachant que l'équipement dédié à cette fonction ne requiert pas beaucoup de puissance.

### **- La solution retenue**

Pour répondre aux attentes exposées par le paragraphe précédent, je choisis de mettre en œuvre une solution fondée sur la mise en œuvre d'un équipement actif de réseau dédié pour réaliser la fonction de routage et sur l'installation d'un ordinateur indépendant équipé d'un firewall logiciel pour la fonction de filtrage

L'équipement actif en charge du routage résoudra également la problématique d'isolation des plates-formes d'instruction par rapport aux stations de consultation en permettant la mise en œuvre des réseaux virtuels (VLAN). L'installation d'un équipement actif dédié pour réaliser la fonction de routage se justifie par le fait qu'une telle configuration est plus performante qu'un routeur logiciel face à un volume de données important ou une forte montée en charge. De plus, les mesures effectuées sur le réseau témoignent d'une activité importante dans ce domaine et celle-ci ne pourra qu'augmenter avec la montée en puissance de l'espace numérique de travail.

A l'inverse, le choix d'un firewall logiciel se justifie par le fait que cette solution est suffisante pour répondre aux besoins de l'activité de filtrage observée.

Ainsi, les modifications à apporter à la configuration existante consistent à mettre en place un routeur dédié et un firewall logiciel, comme le présente le schéma n°21.



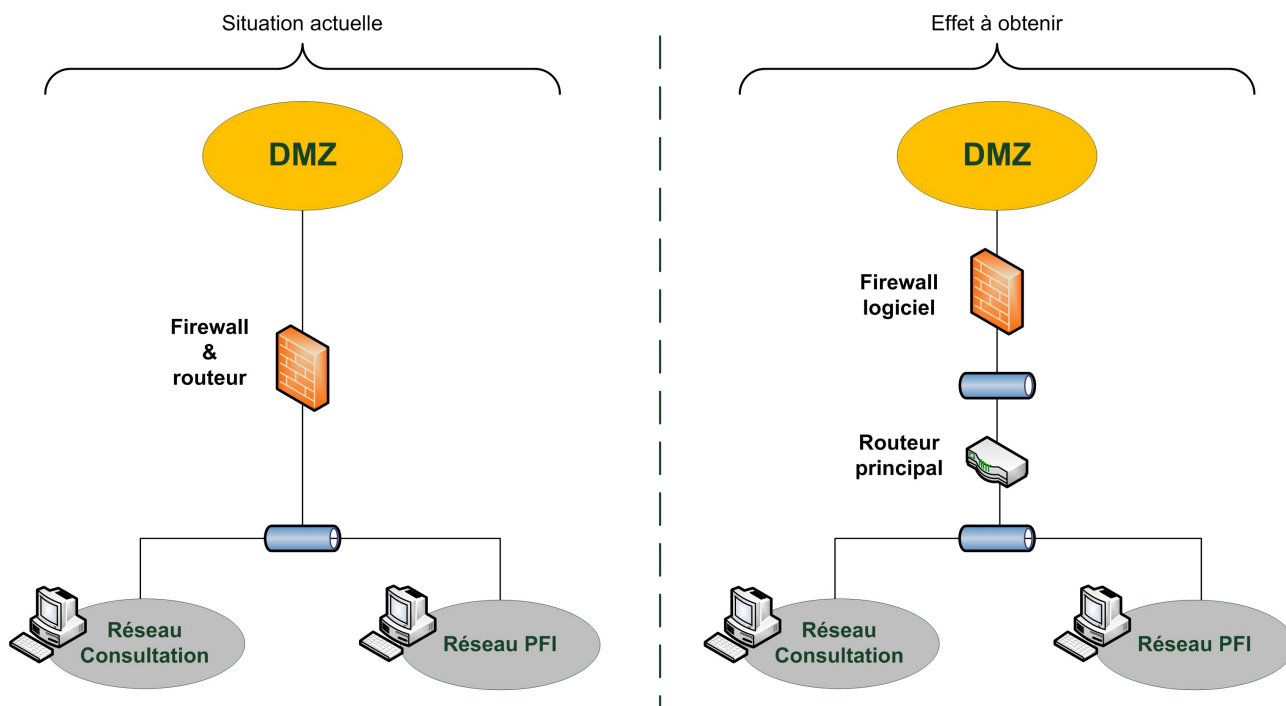


Illustration 21: Amélioration du service d'accès entre les PFI, les stations cadre et la DMZ

La transition vers la solution proposée impose de réaliser **en même temps** la migration vers la nouvelle fonction de routage et de filtrage car l'arrêt de l'équipement précédant, situé en coupure de réseau sous la DMZ, entraînera **une interruption totale** du service d'accès/authentification. Durant cette période, **la capacité à revenir à l'ancienne configuration sera maintenue** afin d'assurer la continuité des services en cas de problème durant le déploiement.

Le prestataire de service principal rattaché aux opérations d'infrastructure des réseaux (DIRISI) est le maître d'œuvre du projet d'isolation logique à base de réseaux virtuels (VLAN) car une telle démarche impose de modifier la configuration de nombreux éléments actifs placés sous sa responsabilité.

Le routeur principal est placé en coupure de réseau sous la DMZ et n'autorise pas une utilisation en mode dégradé. A ce titre, **une sauvegarde régulière de sa configuration** est à réaliser et **un matériel de rechange doit être disponible** afin de rétablir le service dans les meilleurs délais en cas de dysfonctionnement. Cette organisation sera à négocier avec la DIRISI.

La fonction de filtrage est déployée sur un ordinateur doté d'un système d'exploitation Linux Debian et utilise les fonctionnalités de firewall intégrées au noyau du système. Ce choix se justifie par le fait que ce système est performant et **largement utilisé** sur la plate-forme de l'espace numérique de travail. Par conséquent, **les compétences nécessaires à son utilisation sont déjà acquises** par les administrateurs.

Le filtrage est positionné en coupure de réseau et une interruption du service ne permet pas d'envisager un fonctionnement en mode dégradé. Un système de **sauvegarde journalière** est donc à mettre en place pour permettre une restauration du système en cas de dysfonctionnement logiciel.

Pour faire face à une panne matérielle, **un second ordinateur et des cartes réseaux identiques à la configuration de production sont conservés** et tenus à disposition. Un système composé de deux disques durs configurés en miroir est mis en place dans la configuration principale. Ainsi, un



équipement de rechange complet et un disque dur opérationnel et synchronisé avec l'existant seront toujours à disposition des administrateurs. Cette organisation a déjà été préconisée dans la solution traitant de la liaison entre la zone d'hébergement et la DMZ. Il conviendra d'ailleurs d'utiliser le même type d'ordinateur et de carte réseau afin d'optimiser la gestion des stocks de la plate-forme ENT.

### 5.3.e) Liaison n°4 : Serveurs et DMZ

#### - Étude amont

Les serveurs qui fournissent les services nécessaires au fonctionnement de l'espace numérique de travail sont tous connectés à l'architecture technique du système d'information de la formation grâce à une liaison avec la DMZ. La liaison entre ces serveurs et la DMZ est donc **une liaison majeure qui conditionne la disponibilité de l'ensemble de l'espace numérique de travail**.

Pour cette raison, cette liaison doit faire l'objet d'attentions à la hauteur de son importance. Par exemple, il est légitime d'envisager que la liaison soit protégée par un firewall, que les serveurs soient isolés par un système de réseaux virtuels (type VLAN) ou encore qu'ils soient routés grâce à un équipement actif dédié.

Dans les faits, cependant, l'architecture technique actuelle ne met pas en jeu ce découpage. Historiquement, **les serveurs ont été installés dans le même réseau logique que celui des stations de consultation. Ils sont donc rattachés à la liaison étudiée dans le paragraphe précédent** et profitent des mêmes fonctions de filtrage et de routage.

**Cette configuration introduit une faille de sécurité importante dans l'architecture.** En effet, puisque les serveurs évoluent dans le même réseau logique que les stations de consultation, ces dernières peuvent donc y **accéder directement sans filtrage ni routage**. Ainsi, par exemple, une personne malintentionnée pourra lancer depuis une station de consultation une attaque par déni de service<sup>14</sup> vers un serveur sans que celle-ci puisse être stoppée par un firewall. Cette situation n'est pas acceptable car elle met en jeu la disponibilité de l'ensemble de l'espace numérique de travail et donc celle du service de cours en ligne objet de l'expression de besoin de ce mémoire.

Dans le but d'améliorer la qualité du service d'accès/authentification, il est donc nécessaire de procéder à une **isolation des serveurs vis à vis du reste de l'environnement**. Cette transformation peut être réalisée de deux manières : soit la configuration actuelle est conservée et la séparation logique des serveurs est réalisée à l'aide de VLAN, soit une nouvelle liaison est créée en mettant en œuvre un nouveau réseau dans lequel seront intégrés les serveurs. De plus, il est nécessaire d'intégrer **un mécanisme de sécurité interne à chaque serveur** afin d'écarter définitivement le risque d'attaque isolée.

#### - La solution retenue

La solution que je retiens pour fiabiliser la liaison entre les serveurs et la DMZ consiste à créer une nouvelle liaison. Cette liaison sera rendue accessible par une fonction de routage prise en charge par un équipement actif dédié et protégée par une fonction de filtrage installée sur un ordinateur, comme le présente le schéma ci-dessous.

---

<sup>14</sup> Les attaques par déni de service consistent à saturer un serveur en lui adressant de nombreuses requêtes de connexion répétées sur un port donné.

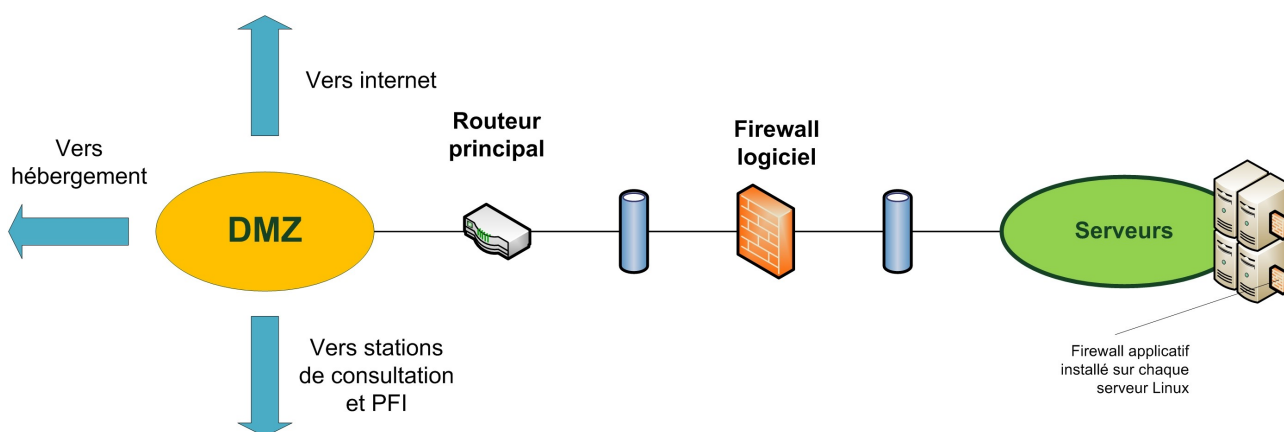


Illustration 22: Nouvelle liaison entre les serveurs et l'environnement

C'est l'importance stratégique de la disponibilité des serveurs qui me conduit à faire le choix d'une solution provoquant la création d'une nouvelle liaison. Ainsi, les serveurs sont indépendants logiquement et physiquement du reste de l'architecture. La solution consistant à configurer des VLAN sur des équipements déjà alloués à la gestion de la liaison avec les stations de consultation et les plates-formes d'instruction n'est pas satisfaisante. Cette solution présente en effet l'inconvénient de **rendre les serveurs trop dépendants de la disponibilité de matériels déjà utilisés pour réaliser une autre liaison.**

La solution retenue met donc en œuvre un routeur et un firewall placés en coupure de ligne sur le réseau. Bien sûr, en cas de panne de l'un de ces éléments, il ne peut y avoir de mode dégradé et le service est interrompu. C'est pourquoi il faudra disposer en permanence d'une **copie de sauvegarde de la configuration des équipements et d'un matériel de rechange à disposition.** Comme pour les solutions retenues avec les liaisons précédentes, l'ordinateur utilisé pour la fonction de filtrage devra mettre en œuvre **un système composé de deux disques durs configurés en miroir** afin de disposer en permanence d'une copie valide du système.

La transition vers la nouvelle solution impose **une coupure totale des services et une modification de la configuration réseau des serveurs.** Pour pallier à un éventuel dysfonctionnement, chacun d'entre eux doit être migré **individuellement** afin de faciliter un retour à la situation initiale en cas de dysfonctionnement.

**Les compétences nécessaires à la réalisation des opérations sont déjà acquises** par les administrateurs du réseau et ne nécessitent pas de formation particulière. Seule une aide à la configuration du routeur principal pourra être demandée à la DIRISI.

La fonction de filtrage est déployée sur un ordinateur équipé d'une distribution Linux Debian et utilise le firewall natif au noyau de ce système nommé « iptables ». Cette configuration est bien représentée sur la plate-forme de l'espace numérique de travail. Tous les serveurs Linux en production reposent déjà sur cette distribution et mettent en œuvre le même firewall avec une configuration adaptée à la nature de chaque service exposé. En conséquence, l'équipe en charge de l'administration du système **dispose déjà des connaissances nécessaires** à l'exploitation de la solution.

Enfin, **une seconde fonction de filtrage est ajoutée à chacun des serveurs** afin de renforcer leurs capacités de protection individuelles. Les machines équipées du système Microsoft Windows activent déjà cette fonction grâce à une extension fournie avec le système antivirus officiel de

l'armée de Terre basé sur la solution Trend Micro. En revanche, les machines équipées d'une distribution Linux (Soit 35 serveurs sur 40 à l'heure de rédaction de ce paragraphe) doivent être dotée d'une solution à définir. Cette fois encore, je retiens le firewall « iptables » pour ses capacités et ses performances. Pour réduire la charge de déploiement des scripts d'initialisation du firewall sur chaque serveur, je prévois l'installation du système « Puppet » (<http://www.puppetlabs.com/>) sur un serveur dédié. Ce système permet de centraliser la configuration de plusieurs machines Linux sur un seul serveur et de déployer chacune d'elles à volonté sans devoir systématiquement prendre le contrôle du serveur concerné. La centralisation des configurations en un point unique permet d'obtenir un contrôle fin des paramètres de fonctionnement et offre la possibilité de répercuter instantanément des modifications sur un ensemble de serveurs en une seule opération.

### **5.3.f) Liaison N°5 : Utilisateurs extérieurs/WAN Internet**

La liaison entre les utilisateurs extérieurs et le WAN Internet permet d'acheminer le réseau Internet au domicile de chacun de ces utilisateurs. Le matériel mis en œuvre pour réaliser cette liaison **dépasse le périmètre d'intervention** de l'ETRS dont le rayon d'action dans ce domaine s'arrête aux frontières de la liaison entre le WAN Internet et la DMZ.

Pour cette raison, et comme cela a été annoncé au début de la conception portant sur le service d'accès et d'authentification, la liaison entre les utilisateurs extérieurs et le WAN Internet ne sera pas traitée dans ce mémoire.

*Cette partie a permis de proposer différentes solutions adaptées à la nature et aux problématiques de chaque liaison entre la DMZ et les zones élémentaires de l'architecture technique du système d'information de la formation.*

*Ainsi, le déploiement d'un nouveau portail captif plus performant est préconisé dans le but de mieux protéger la zone d'hébergement. D'autre part, l'accent est porté sur l'autonomie matérielle et logicielle des différents sous-réseaux physiques ou logiques de l'architecture afin d'améliorer les performances et la sécurité de chacun d'entre eux et de diminuer les conséquences générales en cas d'indisponibilité.*

*La réalisation de ces solutions doit permettre de mettre en œuvre un service d'accès et d'authentification optimisé capable de supporter la montée en charge future du service de cours en ligne.*

## 5.4 : Conception associée au service de cours en ligne

*Cette partie présente la conception des solutions que j'ai réalisées afin d'apporter au service de cours en ligne la capacité à diffuser des flux multimédias pédagogiques.*

*Dans la continuité de la stratégie générale de conception présentée au début de ce chapitre, j'étudie dans un premier temps les zones élémentaires et les liaisons de l'architecture technique générale à prendre en compte dans le cadre de ma conception. Ensuite, pour chacun des éléments identifiés, je propose une solution adaptée.*

### 5.4.a) Les zones élémentaires et les liaisons à prendre en compte

Lors de l'étude du modèle de l'architecture technique générale (voir illustration n°16 de la page 53), nous avons vu qu'il existe deux types majeurs d'éléments :

- Des zones élémentaires qui présentent des caractéristiques techniques hétérogènes,
- Des liaisons qui permettent de relier ces zones élémentaires entre elles.

Le service en charge de la gestion des liaisons est le service d'accès et d'authentification. Il a déjà été traité dans la partie précédente. Si la mise en œuvre des solutions associées au service de cours en ligne nécessite d'apporter des modifications à une liaison, cette action sera réalisée dans le cadre d'un processus ITIL d'amélioration continue rattaché au service d'accès et d'authentification et non à celui du service de cours en ligne. Pour cette raison, je ne prendrai en compte **aucune des liaisons** de l'architecture technique générale dans le cadre de ma conception destinée au service de cours en ligne. Cette exclusion me **garantit ainsi de rester conforme à l'approche ITIL** et me permet de bien **définir le périmètre de la conception** que j'ai à réaliser. De plus, cette approche évite les confusions en écartant la prise en compte de problématiques qui ne concernent pas directement le service visé par le besoin.

Comme cela a déjà été présenté, le service de cours en ligne est déployé dans la zone élémentaire des serveurs et plusieurs serveurs participent à son fonctionnement en lui fournissant des fonctionnalités de stockage de fichiers et de diffusion de type web. Pour la suite de la conception, je dois donc déterminer si seule la zone élémentaire des serveurs est à prendre en compte ou s'il est nécessaire d'inclure d'autres zones. Pour cela, deux scénarios sont possibles :

Le premier consiste à conserver l'organisation actuelle et à privilégier la centralisation des éléments qui participent à la mise en œuvre du service de cours en ligne dans la zone des serveurs. Cette configuration permet de rationaliser les moyens mais introduit le risque de rendre le service de cours en ligne indisponible pour tout le monde en cas d'indisponibilité d'un seul équipement.

Le second scénario possible consiste à redonner le service de cours en ligne au sein de chaque zone élémentaire. Ainsi, les zones sont indépendantes et bénéficient d'une autonomie de fonctionnement. En revanche, les matériels sont dupliqués autant de fois que nécessaire et le volume de donnée à gérer et synchroniser entre zones est plus important.

En regard des deux scénarios présentés précédemment, je fais le choix d'adopter une stratégie qui consiste à continuer à **centraliser la mise en œuvre du service de cours en ligne dans la zone des serveurs**. Pour réduire le risque d'indisponibilité, **je choisis également de mettre en place un mécanisme de haute disponibilité dans la solution déployée** afin de diminuer les probabilités d'une interruption de service. Bien sûr, la centralisation du service de cours en ligne risque de provoquer une augmentation du trafic réseau depuis la zone des serveurs. Toutefois, cette

éventualité d'une augmentation des débits a déjà été prise en compte lors de la conception des solutions apportées au service d'accès et d'authentification. Enfin, le choix d'une installation redondante d'un service de cours en ligne dans chaque zone élémentaire n'est pas opportun en termes de coût de fonctionnement, de charge de maintenance et de risque de désynchronisation des contenus d'une zone à l'autre.

En synthèse, il faut donc retenir que **la phase de conception associée au service de cours en ligne ne traite que de la zone élémentaire des serveurs** de l'architecture générale. Si la mise en production de la solution réalisée n'apporte pas pleinement satisfaction dans une zone élémentaire, il sera toujours possible de revoir la configuration d'une liaison en exécutant un processus ITIL d'amélioration continue rattaché au service d'accès et d'authentification.

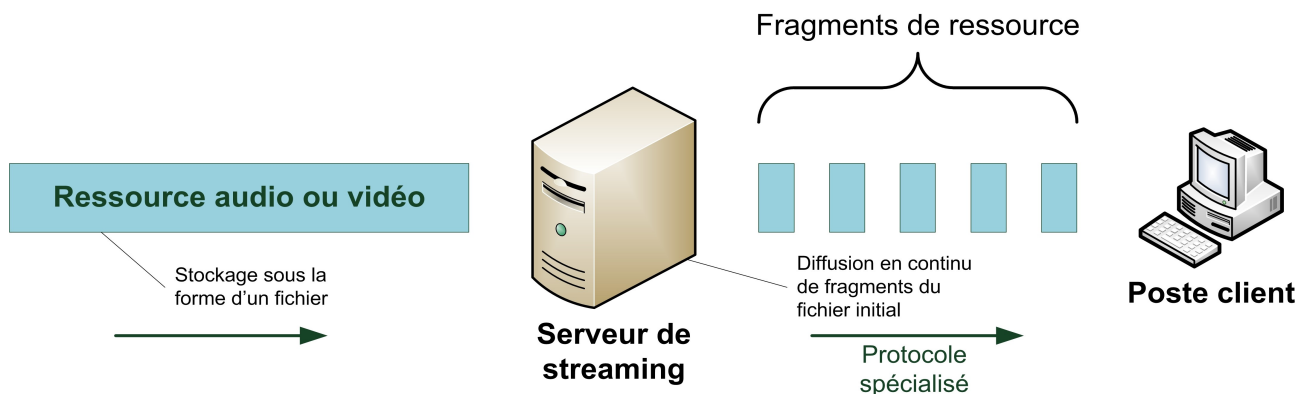
## **5.4.b) Conception de la solution**

### **- Étude amont**

Comme cela a déjà été présenté dans l'étude du besoin, le service de cours en ligne expose des ressources pédagogiques statiques de type page web ou document. Parfois, ces ressources sont enrichies d'une ou plusieurs vidéos. Lorsqu'un utilisateur accède à une ressource pédagogique enrichie, le document s'affiche instantanément dans le navigateur mais la vidéo ne débute qu'après un temps de latence proportionnel à la taille de son fichier et à la distance qui sépare l'utilisateur du serveur.

Ce problème vient du fait que **le service de cours en ligne traite de la même manière tous les types de média** et ne met actuellement en œuvre qu'**une seule stratégie de diffusion basée sur le protocole HTTP**. Le protocole HTTP est le protocole par défaut des communications en mode web. Il est conçu pour transférer une ressource de type fichier en une seule fois entre un serveur et un client. A ce titre, il se prête bien à la diffusion jusqu'à un navigateur des pages web, des documents ou des images de l'espace numérique de travail. En revanche, la consultation d'un média audio ou vidéo est problématique car une ressource de ce type est stockée dans un fichier dont la taille peut varier de quelques dizaines de kilo-octets à plusieurs centaines de méga-octets. Suivant le débit du réseau mis en jeu et la taille du fichier, le téléchargement complet d'une ressource peut alors nécessiter plusieurs minutes et induire un temps de latence entre l'initialisation du transfert et le début effectif de la consultation.

Plusieurs solutions permettent la mise en place d'une stratégie de diffusion adaptée aux médias de type audio ou vidéo. Elles reposent toutes sur le concept de « **streaming** » dont le principe de fonctionnement consiste à **découper un fichier en de nombreux fragments et à les transmettre en continu vers un client via un protocole spécialisé**, comme le présente le schéma suivant.



*Illustration 23: Le principe du streaming de ressource audio ou vidéo*

La consultation d'une ressource en streaming nécessite un lecteur spécialisé ou un plugin de navigateur du côté du client car les fragments transmis par le serveur ne peuvent pas être exploités en l'état. Le rôle du programme client consiste à entretenir une réserve de fragments stockée dans une mémoire cache spécifique et à mettre en jeu une logique de traitement qui permette de restituer la ressource sous sa forme initiale. Pour cette raison, la création d'un site Internet destiné à exposer des ressources en streaming nécessite généralement le développement d'une page web adaptée. Cette page doit alors intégrer un lecteur capable de décoder les flux reçus et être configurée pour interroger le bon serveur de diffusion.

Grâce au streaming, la consultation d'un média peut démarrer instantanément et l'utilisateur peut effectuer des bonds en avant ou en arrière et se positionner là où il le désire au sein de la plage de lecture. Cette souplesse est rendue possible grâce au programme client qui peut interagir avec le serveur et lui transmettre des paramètres sur la nature des fragments à transmettre.

Dans le but d'améliorer la qualité du service de cours en ligne, **il est nécessaire de mettre en place une solution qui implémente les principes du streaming** afin de permettre la consultation des flux multimédias proposés par l'espace numérique de travail.

Il existe plusieurs solutions de streaming disponibles sur le marché. Elle reprennent toutes les principes de fonctionnement énoncés précédemment. Bien sûr, il existe des différences entre les formats de fichiers utilisés ou les spécifications des protocoles, mais globalement, les concepts restent les mêmes. En revanche, toutes ces technologies ne proposent pas les mêmes niveaux de performance et d'intégration. Le tableau ci-dessous présente un aperçu des solutions de streaming actuellement disponibles sur le marché.

<b>Format</b>	<b>Remarque</b>	<b>Solutions serveur</b>	<b>Avantages</b>	<b>Inconvénients</b>	<b>Exemples d'utilisation</b>
Adobe Flash	Conçu pour fonctionner avec le plugin Adobe Flash Player dans un navigateur	Adobe Streaming Serveur, Red5 Server, Wowza media system	- Plugin de navigateur installé sur 97% des machines, - Format open source pris en charge par tous les systèmes, - Streaming adaptatif qui s'adapte au débit du réseau, - Supporte la haute définition.	- Nécessite la conversion des vidéos, - Solutions logicielles commerciales onéreuses (Supérieure à 5 000€).	- Youtube, - Daily Motion.
Advanced Streaming Format	Conçu pour fonctionner avec le logiciel Windows Media Player ou le plugin correspondant dans un navigateur.	Windows Media Server	- Plugin de navigateur fournit en standard avec Windows, - Mise en œuvre aisée, - Streaming adaptatif qui s'adapte au débit du réseau, - Supporte la haute définition.	- Nécessite la conversion des vidéos, - Disponible uniquement dans le monde Windows, - Technologie naissante et peu répandue	- Sites d'entreprise développé avec Microsoft SharePoint, - Produits métiers spécialisés dans la vidéo.
Realmedia	Conçu pour fonctionner avec le logiciel RealPlayer ou le plugin correspondant dans un navigateur.	RealPlayer server (système Helix)	- Format de vidéo populaire, - Technologie répandue et maîtrisée, - Supporte la haute définition.	- Ne s'adapte pas aux caractéristiques du réseau	- Musique à la demande (type Deezer), - Radios web, - Site d'enseignement à distance du CNAM.
QuickTime	Conçu pour fonctionner avec le logiciel QuickTime player ou le plugin correspondant dans un navigateur.	QuickTime streaming server	- Format de vidéo populaire, - Technologie répandue et maîtrisée, - Supporte la haute définition.	- Indisponible sous les systèmes Linux, - Ne s'adapte pas aux caractéristiques du réseau	- Format disponible sur les sites de location de film en ligne.
Microsoft Smooth Streaming	Conçu pour fonctionner avec le plugin Silverlight dans un navigateur.	IIS Smooth Streaming server	- Streaming adaptatif qui s'adapte au débit du réseau, - Technologie performante, - Supporte la haute définition.	- Nécessite la conversion des vidéos, - Disponible uniquement dans le monde Windows, - Technologie naissante	- Sites d'entreprise développé avec Microsoft SharePoint.

Tableau 7: État de l'art des solutions de streaming audio et vidéo

Parmi les technologies présentées, le format Adobe Flash se distingue plus que les autres en raison de sa grande popularité et de sa maturité technologique. De nos jours, quelle que soit la plate-forme informatique employée, il est fréquent de disposer en natif du plugin « Flash » installé avec son navigateur.

Les vidéos du service de cours en ligne sont déjà enregistrées au format Adobe Flash. Historiquement, ce format a été choisi car il offre des taux de compression de données qui permettent déjà de réduire le temps de latence avant le démarrage d'une vidéo même si celle-ci est téléchargée avec le protocole HTTP.

Consciente de ses limitations en termes de capacité de diffusion, l'ETRS est actuellement en cours d'acquisition d'un produit nommé « Sonic Foundry » qui permet la diffusion de vidéos en streaming. Ce produit exploite les technologies Microsoft et diffuse des flux multimédias de type « Advanced Streaming Format » jusqu'aux navigateurs des clients équipés d'un plugin Silverlight. A terme, les nouvelles vidéos produites par l'école seront donc diffusées sous ce format.

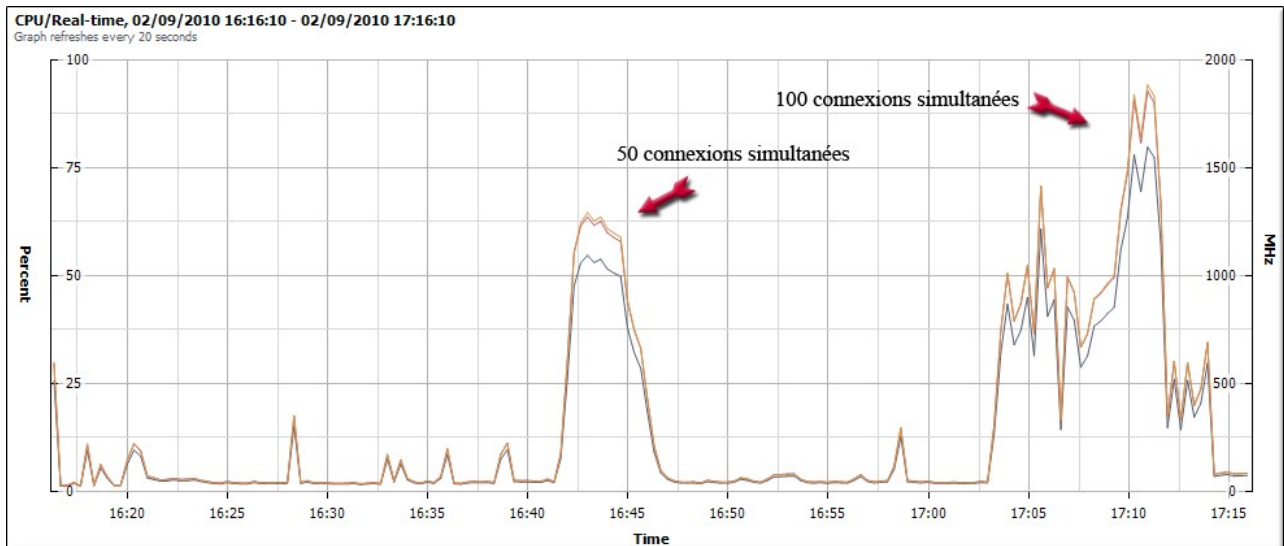
Cependant, et pour des raisons techniques, il n'est pas possible de convertir les vidéos du service de cours en ligne déjà existantes au format Advanced Streaming Format. Cela signifie que **ces médias ne pourront pas bénéficier de la nouvelle solution en cours d'acquisition**. D'autre part, pour des raisons d'économie et comme le souligne une exigence de l'expression de besoin, il n'est pas prévu de reproduire de nouvelles vidéos dont le thème est déjà couvert par un média existant du service de cours en ligne. De ce fait, **la mise en place d'une solution adaptée aux ressources de type Flash Vidéo est nécessaire pour le service de cours en ligne**.

#### **- La solution retenue**

La solution que j'ai retenue pour diffuser les vidéos existantes du service de cours en ligne au format Flash Vidéo consiste à mettre en œuvre une architecture qui exploite les capacités du **serveur de streaming libre Red5**. Ce serveur est déjà utilisé dans de nombreux sites web pour diffuser les flux multimédias générés par une webcam ou pour fournir des vidéos à la demande. Il présente l'avantage d'être gratuit et de supporter le protocole « Real Time Messaging Protocol » (<http://www.adobe.com/devnet/rtmp.html>) défini par Adobe System sur lequel s'appuient les plugins des navigateurs pour restituer les ressources de type Flash Vidéo en diffusion continue.

Le nombre de connexions simultanées susceptibles d'être supportées par la solution est difficile à évaluer car **le service de cours en ligne n'a pas encore connu une utilisation qui permette de collecter des statistiques d'utilisation fiables**. En revanche, j'ai effectué des tests de montée en charge sur un serveur Red5 virtualisé disposant de 2 Go de mémoire vive et doté d'un système Linux. J'ai choisi cette configuration car elle est la plus représentative des serveurs actuellement en production au sein de l'architecture technique de l'espace numérique de travail. A l'aide d'un script que j'ai développé, **le test cumule des connexions consommatrices de flux vidéo** grâce à un utilitaire en ligne de commande qui permet de **simuler le même comportement que celui d'un lecteur multimédia** qui restitue une ressource en streaming. Les résultats font apparaître qu'**il est possible d'envisager une centaine de connexions simultanées** avant d'atteindre une charge d'utilisation des processeurs qui impacte le bon fonctionnement global du système, comme le présente le graphique ci-dessous.





*Illustration 24: Montée en charge des processeurs durant un test de connexions simultanées.*

Comme je l'ai présenté plus haut dans ce chapitre, **le service de cours en ligne est un service critique qui doit mettre en œuvre des mécanismes permettant de réduire les risques d'indisponibilité**. Pour faire face à une fréquence d'utilisation qu'il est encore difficile de connaître et pour continuer à assurer le fonctionnement même en cas de panne d'un serveur de diffusion, je choisis d'intégrer à la solution un **système de répartition de charge de type « load balancing »**. Le principe du load balancing a déjà été présenté lors de la conception de la solution rattachée à la liaison entre le WAN Internet et la DMZ du service d'accès et d'authentification. Le load balancing permet ici d'ajouter à volonté des serveurs de streaming supplémentaires dans l'architecture. Un serveur frontal reçoit les requêtes de consultation des ressources multimédias et répartit la charge de diffusion à l'un des serveurs de streaming qui lui est rattaché. Les résultats du test de montée en charge indiquent qu'il sera nécessaire d'ajouter un nouveau serveur de streaming dès lors que le nombre de connexions simultanées atteindra un nouveau multiple de cent. Grâce à ce système, **l'incertitude relative au nombre de connexions simultanées est traitée**. De plus, **en cas de panne de l'un des serveurs de streaming, le système répartira la charge sur les serveurs restants**, garantissant ainsi une meilleure disponibilité par rapport à une solution basée sur un seul serveur.

Afin de ne pas devoir copier de manière redondante les vidéos à diffuser sur chacun des serveurs utilisés, un système de stockage en réseau de type « Network Attached Storage » (NAS) doit être mis en œuvre afin d'offrir une zone de données partagée.

Enfin, pour valider le bon fonctionnement global de la solution et améliorer la disponibilité, la plate-forme intégrera dès la première mise en service deux serveurs de streaming en répartition de charge et sera donc conforme au schéma d'architecture générale suivant.

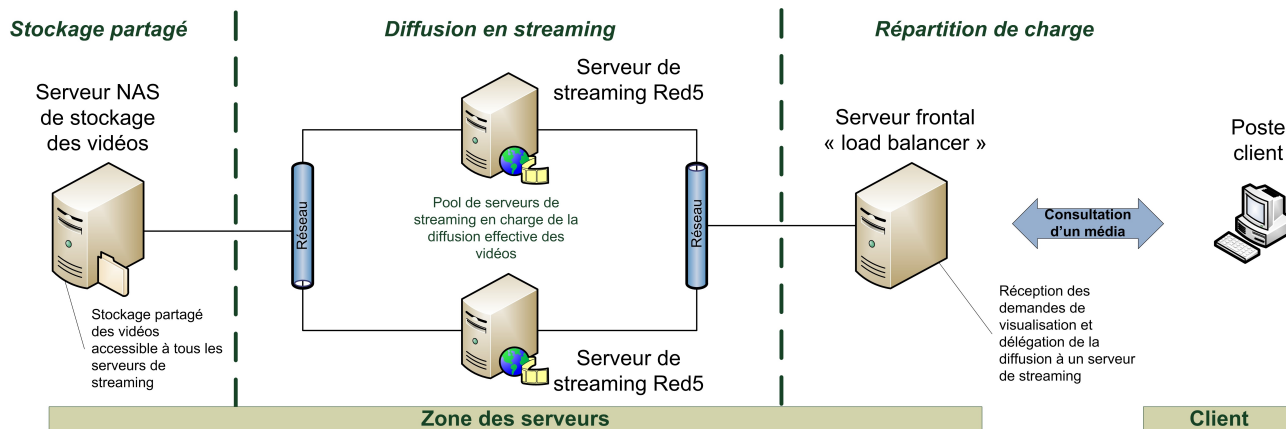


Illustration 25: Architecture générale de la solution de diffusion des vidéos Flash en streaming

La panne de l'un des serveurs de streaming est transparente aux yeux des utilisateurs car le système de répartition de charge confie alors automatiquement la suite de la diffusion à l'un des autres serveurs en activité. En revanche, **l'indisponibilité du serveur frontal provoque l'interruption totale du service**. Les administrateurs veilleront donc à toujours **disposer d'une seconde machine configurée en serveur de répartition de charge** afin de pouvoir la démarrer en cas de panne du serveur principal. Idéalement, cette machine sera virtualisée afin de ne pas provoquer des coûts de conservation inutiles en immobilisant une station physique destinée à rester un élément de rechange.

Cependant, et **pour offrir un mode dégradé en cas de panne du serveur frontal**, une redirection temporaire au niveau du DNS de l'adresse du serveur frontal vers l'un des serveurs de streaming rattaché permettra de fournir une solution d'attente.

Le personnel en charge du serveur frontal et des serveurs de diffusion en streaming doivent disposer **des connaissances de base nécessaires à l'administration des solutions employées**. Pour cela, je prévois la **rédaction d'un document permettant de centraliser les informations indispensables** à connaître. Pour une utilisation plus poussée, la documentation des solutions disponibles sur le site Internet respectif de chacune des solutions constitue une bonne base de départ.

La visualisation d'une vidéo de type Flash en streaming dans un navigateur requiert d'accéder à une page web qui intègre un lecteur multimédia compatible avec le protocole RTMP. Ce lecteur doit de plus pointer vers la ressource à consulter. Pour masquer cette opération, **j'ai développé une page web spécialisée qui intègre le lecteur multimédia libre et open source « FLV Player »** (<http://flv-player.net>). Cette page web doit être appelée depuis un navigateur en spécifiant dans son URL le nom de la vidéo à consulter en streaming. Un code JavaScript développé à cet effet permet alors de faire pointer le lecteur multimédia vers la bonne vidéo grâce à un mécanisme d'analyse de l'URL de la page<sup>15</sup>. La transition vers cette nouvelle solution nécessite uniquement de **modifier les liens vers les vidéos contenues dans les ressources pédagogiques** du service de cours en ligne. Ainsi, **je reste conforme aux exigences et contraintes de l'expression de besoin**.

L'espace de stockage partagé des vidéos est localisé sur un serveur de type NAS. La solution que je propose met en œuvre le produit libre « Open Filer ». Il s'agit d'une distribution Linux complète optimisée pour le stockage de fichiers compatible avec le protocole « Internet Small Computer System Interface » (iSCSI). Le protocole iSCSI permet le transport de commandes matérielles SCSI sur un réseau TCP/IP sécurisé. Ainsi, l'espace de stockage des vidéos pourra être rattaché

15 Le code Javascript et le contenu de la page web sont fournis en annexe 6

directement au système de fichier de chacun des serveurs de streaming sans que ceux-ci aient conscience de la composante distante de la liaison. Les vidéos déposées dans le NAS **devront faire l'objet d'une sauvegarde régulière** afin de pallier à un éventuel dysfonctionnement de l'équipement. En effet, une panne du NAS provoque l'interruption du service de diffusion en streaming. La bascule en mode dégradé est néanmoins possible **en recopiant temporairement** les vidéos sur chacun des serveurs depuis le système de sauvegarde.

Les connaissances nécessaires à l'administration du serveur NAS sont réduites à la compréhension de l'interface d'administration proposée par le système. Cette interface met en avant des notions classiques d'informatique et de réseau déjà maîtrisées par les administrateurs de l'école. Cette fois encore, l'accès à la documentation de la solution depuis son site Internet peut constituer une source d'information supplémentaire.

*Cette partie apporte plusieurs solutions au problème de diffusion saccadée des médias du service de cours en ligne. En premier lieu, une solution reposant sur le concept de diffusion continue est proposée grâce à la mise en œuvre d'un serveur de streaming. Plutôt que de déployer un seul serveur difficile à dimensionner, un système de répartition de charge entre plusieurs serveurs est proposé. Ce système favorise la disponibilité du service de cours en ligne et permet de faire face à une montée en charge par simple adjonction de serveur supplémentaire.*

*Pour éviter de copier autant de fois les vidéos à diffuser qu'il y a de serveurs, un système de stockage partagé en réseau est proposé afin de limiter l'espace nécessaire à l'hébergement des médias.*

*Le déploiement de la solution est centralisé dans la zone des serveurs plutôt que dans chaque zone élémentaire de l'architecture technique générale. Ce choix se justifie par l'économie de moyen réalisée et par le fait que les conceptions proposées précédemment pour améliorer le service d'accès et d'authentification sont prévues pour supporter cette configuration.*

---

*Ce chapitre a permis de présenter la conception des différentes solutions que j'ai réalisées dans le but d'améliorer les capacités de diffusion des flux multimédias de l'espace numérique de travail, conformément à l'expression de besoin.*

*Ma démarche a d'abord consisté à analyser l'architecture technique générale dans laquelle je dois implanter mes solutions. Pour cela, j'ai isolé des zones élémentaires qui présentent des caractéristiques hétérogènes et identifié les liaisons que les flux doivent emprunter pour les atteindre.*

*Ensuite, en conservant l'approche orientée service déjà employée pour gérer le projet CAN/ENT, j'ai identifié les services de l'espace numérique de travail impactés par le projet. Pour chaque service identifié, j'ai alors conçu des solutions en prenant en compte les particularités des zones élémentaires et des liaisons concernées.*

## 6 : RÉALISATION

*Dans la continuité de la phase de conception, ce chapitre présente la phase de réalisation que j'ai menée dans le cadre de mon projet.*

*Une première partie expose le contexte général dans lequel mes actions se sont déroulées ainsi que les difficultés auxquelles j'ai dû faire face. Une seconde partie présente ensuite mes réalisations effectives en conservant l'approche orientée service validée lors de la conception de mes solutions.*

### 6.1 : Contexte général de réalisation

*Au préalable de la description des réalisations que j'ai menées dans le cadre de mon projet, il me paraît nécessaire de présenter le contexte général dans lequel elles se sont déroulées.*

*Dans un premier temps, je rappelle les différentes solutions proposées lors de la phase de conception. Ensuite, je présente les difficultés organiques et organisationnelles qui ont influencé le déroulement des opérations.*

Comme cela a été présenté dans le chapitre précédent, la stratégie de conception des solutions repose sur un découpage à deux niveaux. Le premier niveau couvre les services impactés par le projet et le second traite des liaisons et zones élémentaires de l'architecture technique générale dans lesquelles les solutions doivent s'intégrer (voir l'illustration n°16 de la page 53). En fonction de cette stratégie, le tableau n°8 ci-dessous présente la synthèse des solutions proposées :

Service d'accès et d'authentification	Service de cours en ligne
<b>- Liaison entre WAN Internet et DMZ :</b> Mise en place d'une solution de redondance logique de réseaux Internet.	Mise en place d'une solution de diffusion en streaming.
<b>- Liaison entre zone d'hébergement et DMZ :</b> Mise en place d'un nouveau portail captif.	La solution comprend un système de répartition de charge parmi un pool de serveurs dont le nombre d'éléments peut varier.
<b>- Liaison entre PFI/Consultation et DMZ :</b> Isolation de la liaison à l'aide de matériel dédié.	Les médias diffusés sont centralisés sur un stockage en réseau partagé par tous les serveurs de diffusion.
<b>- Liaison entre serveurs et DMZ :</b> Isolation de la liaison à l'aide de matériel dédié. Déploiement d'une fonction de filtrage personnalisée sur chaque serveur.	

*Tableau 8: Synthèse des solutions à réaliser*

#### **- Difficultés organiques**

Les actions nécessaires à la réalisation des solutions ont parfois dépassé le domaine d'intervention de l'École des transmissions et ont fait l'objet d'une demande de prise en charge par un organisme extérieur. Il s'agit ici de toutes les actions nécessitant la modification ou l'installation des éléments physiques du réseau (switch, routeurs, armoires de brassage, etc.) prises en charge par un opérateur unique dans le cadre d'un contrat de service.

Comme l'a présentée l'étude de l'existant technique, l'organisme en charge de la gestion physique du réseau est la direction inter-armées des réseaux d'infrastructure et des systèmes d'information (DIRISI). Cet organisme est responsable de l'ensemble des réseaux de la base de défense de Rennes et sa charge de travail est considérable en regard de son effectif. Pour cette raison, **seule une partie des actions nécessaires à la réalisation et à la mise en place des solutions qui concernent l'infrastructure du réseau ont pu être planifiées et traitées par la DIRISI**. Dans les faits, je n'ai pas pu finaliser la mise en œuvre des solutions proposées pour isoler physiquement les liaisons à l'aide de matériel dédié ou pour mettre en place la redondance logique de réseaux Internet. En effet, ces solutions nécessitaient de modifier la configuration de tous les équipements actifs de l'école afin de modifier leurs tables de routage ou leur configuration en VLAN. La DIRISI n'a pas eu la ressource nécessaire pour réaliser cette opération qui, selon une évaluation conjointe, aurait nécessité un travail de plusieurs semaines.

### **- Difficultés organisationnelles**

Ma réussite au concours d'ingénieur d'études et de fabrications (IEF) du ministère de la Défense a entraîné ma mutation prématurée de l'École des transmissions le 13 décembre 2010. A cet effet, je n'ai pas pu finaliser moi même le déploiement du portail captif Alcasar que j'avais prévu de mettre en service entre la zone d'hébergement et la DMZ. Cependant, **mes travaux ont été poursuivis** afin de passer en production en mars 2011 l'équipement que j'avais préparé et validé en phase de test.

### **- Bilan**

Finalement, et malgré les points évoqués précédemment, **j'ai pu traiter dans son ensemble l'expression de besoin associée à ce mémoire d'ingénieur** et mettre en œuvre un ensemble de solutions qui permettent d'offrir à l'espace numérique de travail la capacité à diffuser des flux pédagogiques multimédias. C'est pourquoi la suite de chapitre expose les différentes actions que j'ai menées pour réaliser ces solutions. Pour cela, je conserve une approche orientée service et **continue à exploiter le recueil de bonnes pratiques ITIL**. Je l'utilise cette fois pour me guider durant les phases de transition et d'exploitation des solutions déployées.

*Les actions menées pour réaliser les solutions continuent à s'inscrire dans une démarche orientée service et exploitent le recueil de bonnes pratiques ITIL. La suite de ce chapitre prend en compte cette méthodologie et présente les solutions réalisées en fonction du service de destination.*

## 6.2 : Réalisations associées au service d'accès/authentification

Les solutions réalisées pour améliorer le service d'accès et d'authentification ont porté sur deux aspects. Le premier traite de la mise en œuvre d'une fonction de filtrage personnalisée sur chaque serveur de l'architecture technique générale. Le second a pour objectif de protéger la liaison entre la zone d'hébergement et la DMZ en installant le portail captif Alcasar (voir l'illustration n° 18 de la page 62)

Les paragraphes ci-dessous présentent la réalisation de ces solutions.

### 6.2.a) Fonction de filtrage par serveur

#### - Analyses et travaux préparatoires

Le principe général de réalisation d'une fonction de filtrage sur un serveur est **dépendant du système d'exploitation hôte**. Pour le système Windows Server, j'ai choisi d'utiliser le firewall intégré au logiciel antivirus « Trend Micro » que les administrateurs de l'école installent par défaut sur les serveurs. Pour le système Linux, j'ai développé un script utilisant les commandes « iptables » pour personnaliser le comportement de NetFilter.

La stratégie retenue pour déployer la fonction de filtrage sur chaque serveur **intègre la contrainte de ne pas provoquer d'interruption de service**. Pour cela, j'ai d'abord créé une maquette de test en procédant à l'installation de deux serveurs virtualisés exécutant chacun un système d'exploitation différent. J'ai pu alors développer et tester les procédures et les scripts nécessaires à la réalisation et à la mise en place des solutions.

La politique de sécurité par défaut retenue consiste à fermer tous les ports réseau et à n'ouvrir que ceux nécessaires au fonctionnement des services mis en œuvre. Dans ces conditions, la fonction de filtrage n'a que peu d'impact pour un serveur et seule la gestion des fichiers de journalisation requiert l'attention des administrateurs. Sur ce dernier point, je n'ai pas développé de procédure dédiée car les tâches à effectuer sont implicites et maîtrisées par les personnels.

La planification générale des tâches effectuées pour réaliser la solution est représentée par l'illustration n°26.

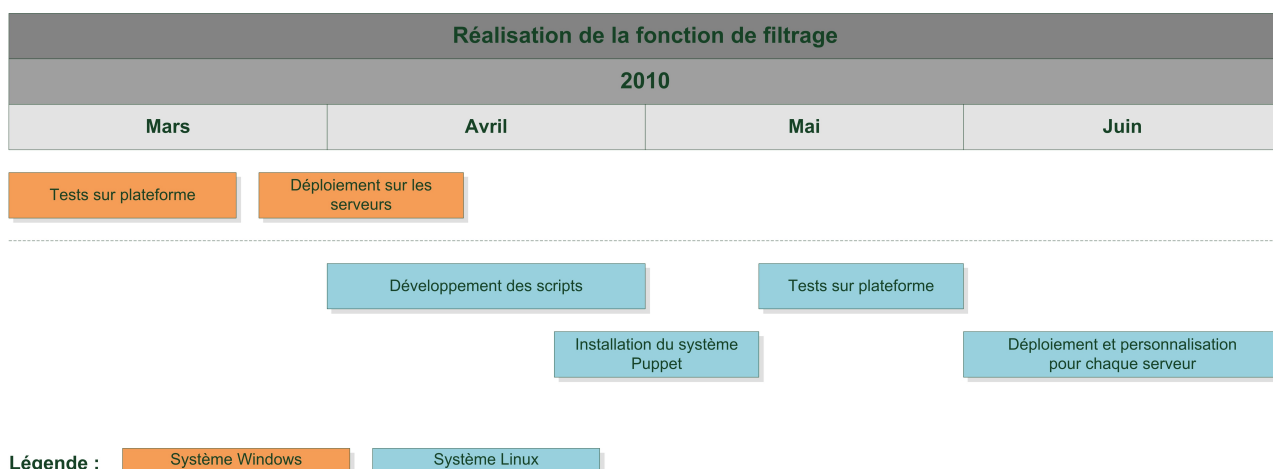


Illustration 26: Planning de réalisation de la fonction de filtrage

Les paragraphes ci-dessous présentent en détail le déroulement des tâches réalisées.

## - Réalisation

La réalisation de la fonction de filtrage pour les serveurs équipés d'un système Windows n'a pas soulevée de difficulté particulière. Fort d'une procédure que j'avais pu **valider sur la maquette de test**, j'ai pu déployer les configurations spécifiques à chaque serveur en utilisant l'interface graphique du firewall. Les opérations réalisées n'ont provoqué ni erreur ni interruption de service.

Pour les serveurs équipés d'un système Linux, le travail a été découpé en plusieurs étapes. En premier lieu, j'ai développé et testé sur la maquette de test un script de configuration de firewall destiné ensuite à être dupliqué sur tous les serveurs à protéger. J'ai organisé ce script de manière à ce qu'il contienne une partie commune à chaque serveur et une partie permettant de personnaliser le comportement du filtrage. Le schéma de principe de ce script est représenté par l'illustration n°27.



*Illustration 27: Principe de fonctionnement de la fonction de filtrage pour système Linux*

Cette organisation est classique sur les systèmes Debian et dérivés. Elle présente l'avantage de permettre la mise à jour des éléments principaux d'un programme sans perdre la configuration associée. Par exemple, ce type d'organisation est présent au sein du package du serveur web Apache. Grâce à un système de boucle de personnalisation, les administrateurs peuvent mettre à jour le serveur web sans perdre la configuration spécifique à chaque site web hébergé.

**Le bloc commun du script intègre la politique de filtrage générale partagée par tous les serveurs.** Il s'agit par exemple de la capacité à accepter la prise de contrôle à distance via le protocole sécurisé SSH, la capacité à répondre aux requêtes de type ICMP (ping) ou encore la possibilité d'utiliser la boucle réseau locale (localhost).

La seconde partie du script intègre **une boucle de personnalisation**. Cette boucle scrute et lit des petits **fichiers de commandes déposés à côté du script principal**. Chaque fichier de commande contient une ou plusieurs instructions «iptables» permettant d'effectuer une action précise comme activer un port particulier ou autoriser un comportement défini. La liste ci-dessous fournit à titre indicatif quelques exemple de fichiers de commandes :

- Fichier de commandes pour autoriser les connexions de type web sur les ports 80 (HTTP) et 443 (HTTPS),
- Fichier de commandes pour autoriser les connexions à un serveur de base de données

- MySQL,
- Fichier de commandes pour autoriser les connexions à un annuaire LDAP.

Sur chaque serveur, il suffit alors de **déposer les scripts de commande qui correspondent à leur configuration** pour personnaliser leur fonction de filtrage.

Le bloc de fin permet de finaliser le script général en appliquant notamment une règle de blocage par défaut. A ce stade, **toute tentative de connexion qui n'a pas été explicitement autorisée par le bloc commun ou la boucle de personnalisation est systématiquement rejetée.**

Sur chaque serveur, le script de configuration de la fonction de filtrage est appelé au démarrage du système. **Pour renforcer la sécurité**, il est également **rechargé automatiquement toutes les heures** grâce à une tâche planifiée de type « cron<sup>16</sup> ». Grâce à ce mécanisme, **le script est garant de la configuration de la fonction de filtrage** et permet d'éliminer périodiquement les modifications qui pourraient être réalisées par un administrateur distrait ou une personne mal intentionnée.

Le déploiement de la fonction de filtrage impose de copier le script de configuration et les scripts de commande sur chaque serveur. Cette manipulation peut se révéler fastidieuse et répétitive avec le nombre grandissant de serveurs à administrer et, par expérience, les évolutions de configuration prévisibles. Pour remédier à cet inconvénient, j'ai prévu, lors de la conception, la mise en place d'un système permettant de **centraliser la configuration de chacun des serveurs en un point unique et de la déployer automatiquement par le réseau**. J'ai utilisé pour cela le système « Puppet » (<http://www.puppetlabs.com>) qui fonctionne en mode client/serveur. Le serveur centralise les fichiers de configuration et le client installé sur chaque serveur à gérer interroge régulièrement le système pour connaître les modifications à apporter et pour les importer le cas échéant au sein d'un flux chiffré.

En installant le client Puppet sur chacun des serveurs concernés par le déploiement, j'ai pu centraliser en un seul endroit toutes les configurations de fonction de filtrage des serveurs que je souhaitais protéger. Ce système a permis ensuite de simplifier considérablement les tâches d'administration des serveurs lorsque des évolutions nécessitaient de modifier leur configuration. Des informations techniques supplémentaires sur le système Puppet et le script de configuration de la fonction de filtrage sont fournies en annexe III.

Les actions réalisées pour **tester la solution** ont consistées à utiliser la commande Linux « Telnet ». Telnet est avant tout un protocole qui permet de prendre le contrôle à distance d'une machine. La commande s'utilise en spécifiant une adresse IP et accessoirement un numéro de port. Grâce à cette commande, j'ai pu vérifier que les ports des serveurs étaient bien ouverts ou fermés selon la configuration choisie de la politique de filtrage. Des tests complémentaires ont également été réalisés avec le programme nmap (<http://nmap.org>) qui permet de scanner en interne et en externe l'ensemble des ports d'un serveur et obtenir ainsi un état de sa configuration réseau. Enfin, durant la phase de production, j'ai opéré à un contrôle régulier des fichiers de journalisation des firewalls sans toutefois constater d'anomalie à signaler.

---

16 « cron » est le programme de référence des systèmes Linux pour exécuter des tâches planifiées. Ses possibilités de configuration sont très étendues et permettent le réglage de planifications complexes.



## - Amélioration continue et perspectives d'évolution

Le système de script utilisé pour réaliser la fonction de filtrage sur les serveurs Linux est souple et adaptable. De ce fait, il est possible d'envisager une évolution visant à ajouter des commandes favorisant non plus le filtrage mais aussi la gestion de la qualité de service.

Sous Linux, c'est le programme « tc »<sup>17</sup> qui prend en charge ce type de paramétrage. Cette commande permet notamment de définir des priorités sur les flux. Ainsi, pour un serveur web, on pourra par exemple privilégier les flux entrants et sortants sur les ports 80 (HTTP) et 443 (HTTPS) et rendre tous les autres flux moins prioritaires. Sur le même principe, un serveur de base de données ou un serveur de fichier pourront définir des priorités de flux permettant de privilégier les services qu'ils exposent.

La gestion de la qualité de service est également disponible sur le système Windows mais la solution que j'ai utilisée pour implémenter la fonction de filtrage n'offre pas ce type de paramétrage. Si cette évolution devait être réalisée, il faudrait donc prévoir la mise en œuvre des fonctions de bases natives au système ou faire l'acquisition d'un logiciel plus évolué tel que « NetLimiter » (<http://www.netlimiter.com>) ou équivalent.

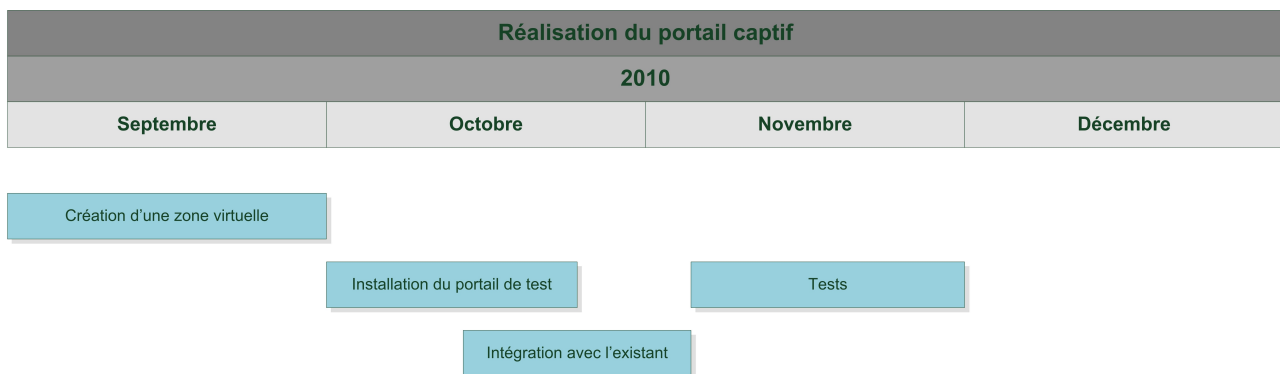
### 6.2.b) Installation du portail captif Alcasar

#### - Analyses et travaux préparatoires

Un portail captif a pour **objectif de protéger la liaison ente la zone d'hébergement et la DMZ** de l'école. Le matériel mis en œuvre repose sur un ordinateur équipé de deux cartes réseaux que l'on positionne en coupure de réseau du coté de la DMZ.

**La stratégie générale** que j'ai retenue pour réaliser cette solution a consisté à **créer une zone virtuelle de test** au sein de l'architecture technique générale et de relier cette zone au reste du réseau grâce au portail captif en cours d'installation. J'ai pu ainsi simuler d'une manière aussi proche que possible de la réalité les différentes situations que le portail devrait gérer un fois en situation opérationnelle. La dernière phase de cette stratégie consistait à déployer en production l'équipement validé en phase de test.

La planification générale des tâches effectuées pour réaliser la solution est représentée par l'illustration n°28.



*Illustration 28: Planning de réalisation du portail captif*

<sup>17</sup> Le nom de commande **tc** est une contraction qui désigne ici le terme « Traffic Control » (contrôle du trafic)

Les paragraphes ci-dessous présentent en détail le déroulement des tâches réalisées.

### - Tests et simulation

La mise en œuvre d'un portail captif est une **opération critique vis à vis de la sécurité informatique**. En effet, si le portail n'est pas bien configuré, il peut permettre des connexions illicites ou introduire de graves failles de sécurité dans le système. Pour me permettre de préparer l'installation d'un nouveau portail captif en ayant **recours à une gestion des risques mesurée**, j'ai choisi de simuler une zone d'hébergement virtuelle et de la relier à la DMZ grâce au nouveau portail captif en cours de réalisation.

Pour simuler les clients situés dans la zone d'hébergement, j'ai connecté un ordinateur portable à la carte réseau interne du portail captif. Cet ordinateur portable était équipé d'une distribution Linux Ubuntu (<http://ubuntu-fr.org>) et du logiciel de virtualisation VirtualBox (<http://www.virtualbox.org>) avec lequel j'ai créé et exécuté une machine virtuelle équipée du système d'exploitation Windows XP. Cette configuration m'a permis ainsi de **simuler deux clients situés dans la zone d'hébergement virtuelle** et exécutant chacun un système d'exploitation différent. L'illustration n°29 présente le schéma de principe de la plate-forme de test créée pour les besoins de la réalisation et offre un aperçu de son intégration au sein de l'architecture technique générale.

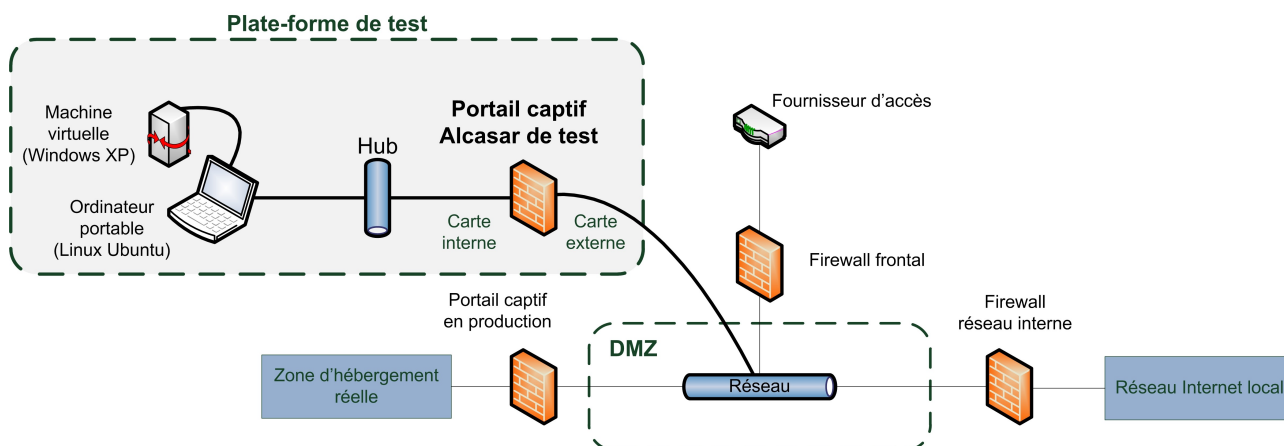


Illustration 29: Plate-forme de test pour l'installation du portail captif

Grâce à la machine virtuelle embarquée et à l'ordinateur portable, **j'ai pu simuler de nombreux comportements représentatifs des actions réellement effectuées dans la zone d'hébergement** comme par exemple la création d'une nouvelle connexion, la navigation vers le réseau Internet ou vers l'espace numérique de travail ou encore le téléchargement de fichier. D'autre part, **j'ai pu tester les dispositifs de sécurité intégrés du portail Alcasar** en configurant par exemple la même adresse IP pour le poste Linux et le poste Windows et en vérifiant que le portail détectait bien une tentative d'usurpation d'identité et protégeait le réseau en coupant les connexions. A titre d'exemple, ce mécanisme d'exclusion n'est pas proposé par l'équipement actuellement en production.

### - Intégration avec l'existant

Comme cela avait été annoncé lors de la phase de conception, j'ai couplé le portail Alcasar à l'annuaire LDAP utilisé par la centrale d'authentification CAS de l'espace numérique de travail. Ainsi, les utilisateurs doivent exploiter les mêmes noms de connexion et mots de passe que ceux utilisés pour se connecter à l'espace numérique de travail. Je reviendrai plus bas sur les nouvelles possibilités offertes par cette configuration.

Le couplage avec l'annuaire LDAP a nécessité quelques modifications dans la configuration du firewall protégeant le réseau interne de l'école afin de laisser circuler librement les requêtes d'interrogation vers le serveur associé. Dans le même esprit, l'intégration du nouveau portail captif au sein du réseau a nécessité d'ajouter des règles dans les différents firewalls de la DMZ afin de **pouvoir reproduire les mêmes flux que ceux déjà autorisés pour l'ancien équipement**. Cette action n'a pas présenté de difficulté particulière puisqu'il a globalement s'agit de recopier à l'identique les règles que j'avais déjà administrées avec l'ancien portail.

### **- Installation du portail**

L'installation du portail captif Alcasar est simple et prévue pour être réalisée par une personne ne disposant pas de compétences évoluées en informatique. La procédure est très bien documentée et se décompose en deux phases majeures :

La première consiste à **installer le système d'exploitation qui supporte le portail captif** sur sa machine hôte. Il s'agit ici d'une distribution Linux type « Mandriva » (<http://www.mandriva.com/fr>). Le programme d'installation natif à cette distribution guide étroitement l'utilisateur durant la totalité du processus.

La seconde phase de l'installation consiste à **déployer le portail Alcasar**. Les concepteurs de cette solution fournissent pour cela un script qui prend en charge la totalité de l'opération. Seules quelques questions élémentaires sont posées à l'utilisateur comme la plage d'adresse IP à utiliser ou le nom à donner à la machine hôte. Lors de l'exécution du script d'installation, le système Linux est automatiquement mis à jour à partir du réseau Internet et un certificat de sécurité SSL est automatiquement généré.

Comme annoncé plus haut dans ce chapitre, je n'ai pas pu finaliser le déploiement du portail captif Alcasar en raison de ma mutation après concours. Cependant, **la stratégie d'installation initiale en simulant une zone d'hébergement virtuelle a permis de disposer d'un équipement prêt à passer en production**. De plus, j'ai transmis les connaissances nécessaires à la finalisation du déploiement aux administrateurs en charge de la continuité des actions. L'état d'avancement des travaux permettait finalement d'effectuer la bascule en production après l'exécution de ces trois tâches :

- Remplacement du certificat de sécurité SSL généré automatiquement lors de l'installation d'Alcasar par le certificat de sécurité officiel (auth.ent-etr.net) acheté par l'école auprès de l'organisme de certification Thawte (<https://www.thawte.fr>).
- Renommage du nom de machine du portail pour lui affecter le même nom que celui couvert par le certificat officiel (soit auth.ent-etr.net),
- Raccord du nouveau portail captif à la vraie zone d'hébergement en connectant le câble relié à la carte réseau interne de l'ancien équipement à la carte réseau interne du nouvel équipement.

### **- Amélioration continue et perspectives d'évolution**

Comme tout système technique, la mise en production du portail Alcasar révélera forcément un jour ou l'autre la nécessité de modifier un paramètre ou de répondre à une demande d'évolution. L'un des avantages de ce portail est que son interface graphique d'administration permet d'effectuer l'ensemble des configurations nécessaires à son utilisation. De plus, l'architecture du système repose sur des outils connus et éprouvés qui appartiennent tous au monde du logiciel libre. Les personnels en charge de l'administration du portail connaissent déjà les logiciels et techniques mis

en œuvre. Cette situation permet d'envisager de bonnes perspectives d'évolution et d'amélioration continue.

Une autre raison pour laquelle j'ai choisi le portail Alcasar est que la majeure partie des personnes qui participent à son développement sont présentes à l'École des transmissions. Cette caractéristique permet d'envisager des modifications en profondeur du portail. C'est pourquoi j'ai fait le choix de connecter le portail Alcasar au même annuaire LDAP que celui utilisé par la centrale d'authentification CAS de l'espace numérique de travail. À terme, une évolution majeure bénéfique pour l'École des transmissions consistera à fusionner en une seule les deux phases d'authentification nécessaires à l'obtention d'une connexion depuis la zone d'hébergement puis auprès de l'espace numérique de travail. Un tel mode de fonctionnement n'est pas garanti avec une autre solution au code propriétaire tel le système qui était utilisé jusqu'ici.

*Les travaux effectués pour réaliser les solutions destinées à améliorer le service d'accès et d'authentification ont permis de renforcer et de sécuriser le réseau. Cette amélioration participera indirectement à la fiabilisation et à la pérennité du service de cours en ligne au cœur de l'expression de besoin de mon mémoire.*

*Pour cela, j'ai d'abord réalisé une solution qui contribue à protéger tous les serveurs de l'école grâce à une fonction de filtrage personnalisée. Pour les serveurs Linux, j'ai mis en place une solution qui permet de centraliser en un point unique la configuration de chaque serveur et de la déployer ou la mettre à jour par le réseau.*

*Ensuite, j'ai installé le portail captif Alcasar et je l'ai configuré pour qu'il puisse protéger plus efficacement que cela n'est fait actuellement la liaison entre la zone d'hébergement et la DMZ. Ma mutation prématurée de l'école ne m'a pas permis de finaliser ce travail mais je laisse derrière moi un équipement prêt à passer en production sous réserve de la réalisation de trois actions simples et commentées.*

## 6.3 : Réalisations associées au service de cours en ligne

Les solutions réalisées pour améliorer le service de cours en ligne ont permis de mettre en œuvre une plate-forme de diffusion de vidéo en streaming. L'architecture retenue comprend un mécanisme de répartition de charge entre différents serveurs de diffusion et un stockage partagé des ressources. Du côté du client, une page web a été développée pour simplifier l'accès et la consultation des médias.

Les paragraphes ci-dessous décrivent la réalisation de ces solutions.

### - Planification et travaux préparatoires

Comme cela a déjà été présenté lors de la phase de conception et synthétisé par l'illustration n°25 de la page 77, le **principe général** de réalisation de la solution proposée repose sur **un modèle de fonctionnement à quatre couches** qui traitent chacune une problématique donnée :

- La **répartition de charge**. C'est la capacité à proposer à l'utilisateur un point d'accès unique au système de diffusion des flux multimédias alors que les traitements sont en réalité effectués par plusieurs serveurs,
- La **diffusion en streaming**. Il s'agit ici de la mise en œuvre effective de la diffusion des médias.
- Le **stockage partagé des médias**. Cette solution a été mise en place afin de ne pas dupliquer les médias autant de fois qu'il y a de serveurs de diffusion.
- L'**accès client**. La consultation d'un média en streaming nécessite une solution adaptée côté client pour décoder les flux multimédias.

Pour faciliter l'intégration des couches, j'ai pris soin de **commencer par celles qui étaient autonomes pour finir par celles qui avaient une dépendance avec au moins une autre**.

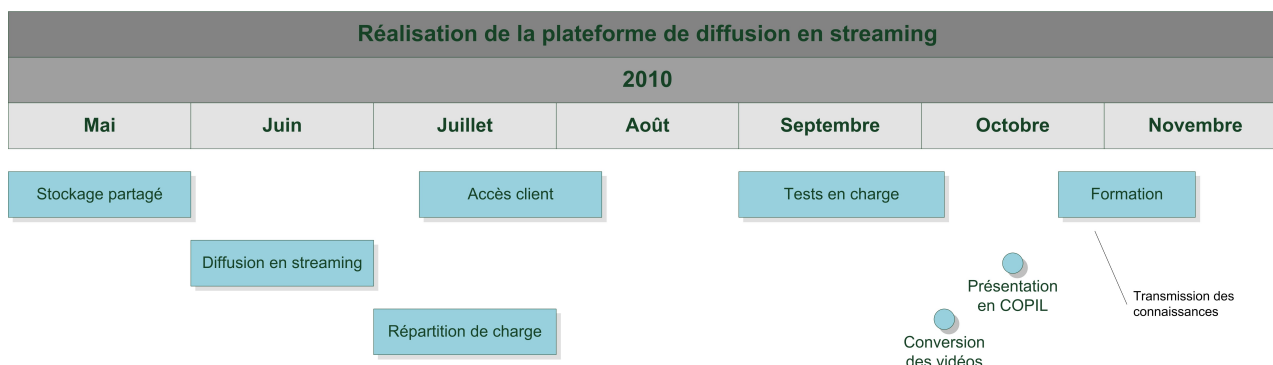
Couche	Dépendance
Répartition de charge	Diffusion en streaming
Diffusion en streaming	Stockage partagé
Stockage partagé	Néant
Accès client	Répartition de charge

Tableau 9: Dépendances entre couches de la plate-forme de diffusion en streaming

En fonction de l'analyse de dépendance synthétisée par le tableau n°9 précédent, j'ai donc choisi de réaliser les couches dans l'ordre suivant : Stockage partagé, diffusion en streaming, répartition de charge et accès client. Cet ordre est en effet naturel en regard du fait que chacune des couches dépend de l'existence de la précédente.

La **stratégie générale** que j'ai retenue pour réaliser la solution s'est appuyée sur **deux étapes**. La première a consisté à créer une plate-forme qui soit **capable de diffuser en streaming les mêmes médias** que ceux proposés par le service de cours en ligne. La seconde étape a consisté à **transmettre les connaissances** nécessaires à la modification des liens vers un média inclus dans les ressources pédagogiques du service de cours en ligne afin qu'ils pointent vers le média équivalent diffusé en streaming. **Une telle stratégie ne nuit pas à la disponibilité du service de**

**cours en ligne.** La modification des liens peut être étalée selon un rythme choisi et supporter une période temporaire durant laquelle l'ancienne et la nouvelle solution sont en production conjointement. La planification générale des tâches effectuées pour réaliser la solution est représentée par l'illustration n°30 ci-dessous.



*Illustration 30: Planning de réalisation de la plate-forme de diffusion en streaming*

L'évaluation du changement à prévoir concerne le format des médias. En effet, un fichier contenant une vidéo destinée à être diffusée en streaming Flash doit être enregistré selon un format spécifique. Les vidéos du service de cours en ligne **ne sont pas compatibles avec ce format et nécessitent une étape d'adaptation**. L'une des actions à mener durant la réalisation de la solution consiste donc à **convertir toutes les vidéos existantes** afin de les rendre exploitables par la plateforme de diffusion.

Il n'existait pas de solution de diffusion en streaming déjà en place au sein de l'architecture technique générale, je n'ai pas eu à prendre en compte de contrainte de continuité de service. D'autre part, le déploiement de la solution n'a pas nécessité de modifier le paramétrage du réseau. Pour ces raisons, **j'ai choisi de ne pas créer de plate-forme de test et de réaliser directement la solution dans sa configuration de production**. J'ai tout de même mis en place une **politique de gestion des risques** en personnalisant la fonction de filtrage<sup>18</sup> de chacun des serveurs créés afin qu'ils ne puissent communiquer qu'avec leurs serveurs dépendants. Par exemple, les serveurs de diffusion ont été configurés pour que seul le serveur de répartition de charge puisse y accéder. Dans le même esprit, le serveur frontal en charge de la répartition de charge a d'abord été configuré pour que seule ma station de travail puisse y accéder avant d'ouvrir l'accès à tous.

Le **périmètre** dans lequel s'inscrit la réalisation de la solution est limité aux seules vidéos **déjà en production au sein du service de cours en ligne**. L'objectif à atteindre, à terme, consiste à pouvoir diffuser toutes ces vidéos en streaming. **La stratégie de retrait** de l'ancienne solution se limite à la **suppression des médias stockés sur le serveur web du service de cours en ligne**. En effet, lorsque tous les liens inclus dans les ressources pédagogiques pointeront vers une ressource diffusée en streaming, les anciens fichiers vidéos qui étaient téléchargés avec le protocole HTTP seront devenus inutiles.

**Les rôles et les responsabilités** sont partagés entre la cellule architecture du bureau de formation assisté par ordinateur (BFAO) pour la prise en charge de l'aspect technique du projet et le bureau enseignement numérique et simulation (BENS) pour la modification des supports pédagogiques impactés par la mise en œuvre de la solution. Mon rôle au sein de cette organisation consiste à faciliter les relations entre ces deux niveaux d'intervention et à proposer une assistance à maîtrise

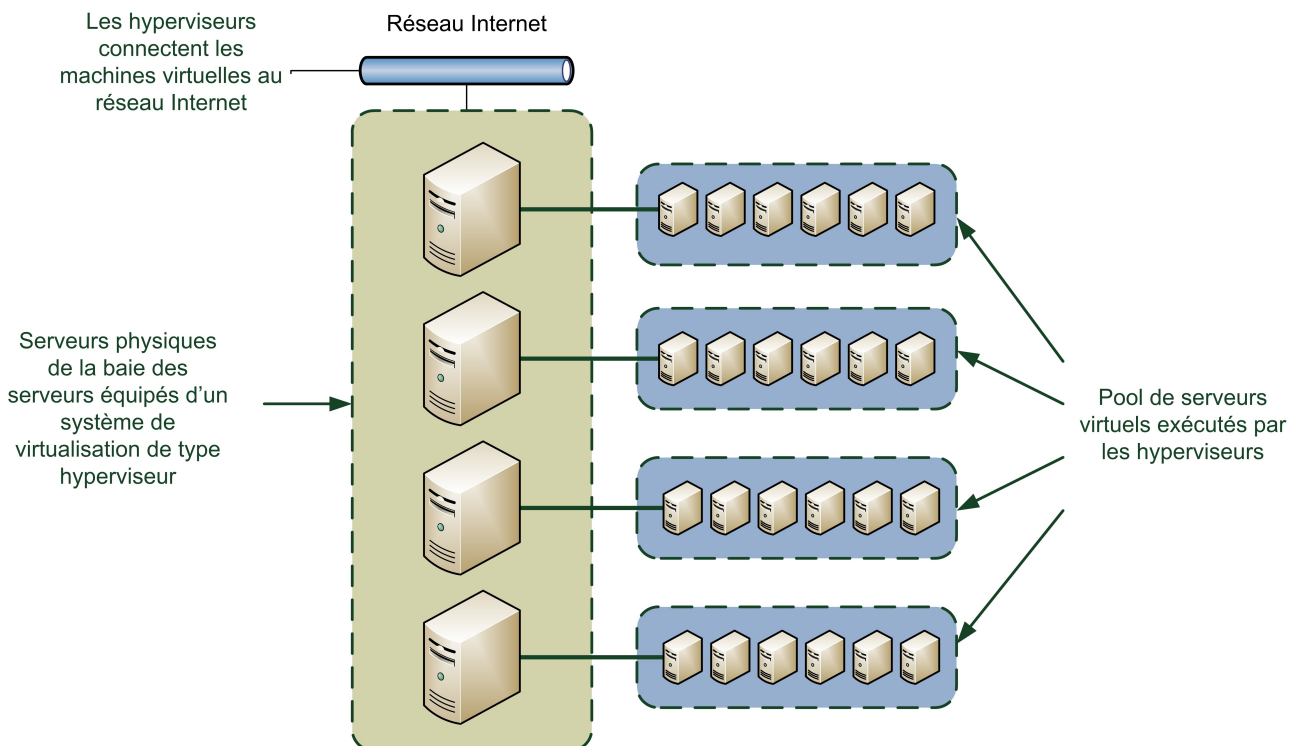
<sup>18</sup> Les serveurs mis en place dans le cadre de cette solution ont été installés avec un système d'exploitation de type Linux et ont intégré la fonction de filtrage personnalisable réalisée dans la partie précédente de ce chapitre.

d'ouvrage aux fonctionnels en charge de la modification des supports pédagogiques.

## - Réalisation

Toutes les solutions présentées ci-dessous ont été réalisées en utilisant le matériel connecté au réseau Internet de la salle des serveurs de l'École des transmissions. On y recense **trois serveurs physiques indépendants** sur lesquels sont installés les firewalls et le portail captif qui protège la liaison entre la zone d'hébergement et la DMZ. **Une baie de six serveurs** de marque Dell montés en rack est également présente. Chaque serveur de la baie est équipé de quatre processeurs et dispose de 24 Go de mémoire vive.

Les travaux réalisés en tant que chef de la cellule architecture du BFAO<sup>19</sup> m'ont conduit à mettre en place **une plate-forme de virtualisation sur quatre des six serveurs de la baie**. Les outils de virtualisation utilisés sont des hyperviseurs ESXi de la marque VMWare (<http://www.vmware.com/fr>). Cette plate-forme permet d'exécuter plusieurs machines virtuelles sur chacun des hyperviseurs et de les connecter au réseau comme s'il s'agissait de serveurs physiques traditionnels, comme le présente l'illustration n°31. Peu avant mon départ de l'École des transmissions, la plate-forme de virtualisation exécutait une quarantaine de serveurs tous nécessaires au fonctionnement ou au test de l'espace numérique de travail.



*Illustration 31: Schéma de principe de la baie de serveurs virtualisés*

La virtualisation est un vaste sujet qui dépasse le périmètre de ce mémoire. Retenons cependant que l'un de ses principaux avantages réside dans la mutualisation et l'économie de moyens physiques qu'elle permet de réaliser. Par exemple, l'exécution de plusieurs serveurs virtuels sur un serveur physique provoque un gain de place considérable dans une salle informatique et permet de réaliser des économies d'électricité. De plus, on constate généralement que le processeur d'un

<sup>19</sup> Mon rôle de chef de la cellule architecture du BFAO a été explicité au chapitre III lors de l'étude de l'existant technique.



serveur physique n'est pas sollicité à hauteur de ses capacités. En répartissant la puissance de calcul entre plusieurs serveurs virtuels, la virtualisation permet de mieux exploiter les équipements et rentabilise ainsi les coûts d'acquisition. D'autre part, une plate-forme virtualisée ne gère pas le réseau de la même manière qu'un serveur traditionnel. Par exemple, **un hyperviseur met en œuvre simultanément toutes ses cartes réseau** quel que soit le nombre de machines virtuelles hébergées et leur configuration respective. Ce mécanisme améliore la disponibilité des services puisque la redondance des cartes permet de pallier l'indisponibilité de l'une d'entre elles. Dans un mode de fonctionnement plus fin, on peut également affecter une ou plusieurs cartes réseau à la gestion des flux entrants et d'autres cartes à la gestion des flux sortants et améliorer ainsi sensiblement les performances du réseau.

Dans le cadre des travaux liés à la réalisation de la solution destinée au service de cours en ligne, j'ai utilisé la plate-forme de virtualisation présentée précédemment. Hormis pour l'installation de la couche de stockage partagé sur laquelle je reviendrai au prochain paragraphe, l'ensemble des nouveaux serveurs nécessaires à la réalisation de la plate-forme de streaming ont été virtualisés. Pour cette raison, il ne sera pas fait état de l'installation d'un équipement quelconque car **le matériel était déjà présent**, installé et opérationnel dans la salle des serveurs.

La **couche de stockage partagé** a été déployée en installant la solution libre OpenFiler (<http://www.openfiler.com>) sur l'un des serveurs **non virtualisés** de la baie que j'avais réservé à cet effet. Avant l'installation de la solution, j'ai ajouté au serveur trois disques durs supplémentaires de 400 Go chacun. En comptant les disques déjà présents, j'ai pu disposer ainsi d'un volume total de 2 To configuré en RAID 5. J'ai choisi de ne pas virtualiser ce serveur en raison du fait que la totalité de l'espace disque lui était alloué et que le volume correspondant était de grande taille. Virtualiser un tel serveur aurait compliqué les procédures relatives à sa sauvegarde et n'aurait pas apporté de plus-value particulière puisqu'il ne restait plus de place disponible pour exécuter d'autres serveurs virtualisés.

Le site web de la solution OpenFiler propose au téléchargement un fichier ISO qui, une fois gravé sur un CD-ROM, peut être utilisé pour démarrer un serveur physique et le configurer en système NAS. OpenFiler fonctionne sur la base d'un noyau Linux compilé et optimisé pour la gestion des fichiers et des communications en réseau.

Une fois le système installé et opérationnel, j'ai utilisé l'interface d'administration pour créer un volume de stockage partagé destiné à contenir les vidéos du service de cours en ligne. J'ai créé ce volume afin qu'il soit compatible avec le protocole iSCSI. Comme cela a été vu lors de la phase de conception, le protocole iSCSI permet de faire transiter des commandes matérielles SCSI par réseau et se prête donc au montage de volume partagé distant. **Pour sécuriser les accès**, j'ai mis en place le **mécanisme de protection** de type Challenge Handshake Authentication Protocol (CHAP) natif au protocole iSCSI. Ce mécanisme impose aux clients une authentification préalable auprès du serveur NAS en présentant un mot de passe. Nous verrons plus bas dans ce chapitre que seuls les serveurs de streaming ont eu connaissance de ce mot de passe et ont pu accéder au volume partagé.

Les hyperviseurs sont reliés au réseau de l'école grâce à deux équipements actifs fixés dans la partie haute de la baie des serveurs. Le serveur physique utilisé pour déployer la solution OpenFiler se situe également dans cette baie. A ce titre, j'ai donc utilisé l'un des équipements actifs de la baie pour relier la couche de stockage partagé aux hyperviseurs. **Cette architecture permet d'obtenir des performances réseau élevées** car seul un équipement actif participe à la liaison et la totalité des éléments électroniques mis en œuvre supportent un débit de 1 Gbits/sec.



La **couche de diffusion en streaming** a été déployée en utilisant la solution libre de diffusion en streaming RED5 (<http://code.google.com/p/red5>). Comme annoncé lors de la phase de conception, **j'ai déployé deux serveurs de diffusion** pour permettre la mise en place du système de répartition de charge. **Chaque serveur de diffusion a été virtualisé et installé dans un hyperviseur différent** afin de garantir l'indépendance physique entre hyperviseurs et assurer la continuité de service même en cas de dysfonctionnement de l'un d'eux.

Les serveurs de diffusion ont été installés avec une distribution Linux Debian et configurés pour être capables d'initier une connexion de type iSCSI vers un volume distant. Cette opération n'a pas présenté de difficulté particulière car ce type de connexion est pris en charge par le système après installation d'un seul paquetage. Une action de paramétrage a été nécessaire afin de spécifier au système l'adresse du serveur NAS à utiliser, le nom du volume à monter et, dans le cas de cette réalisation, le mot de passe CHAP à présenter au serveur pour autoriser la connexion. Une fois la connexion iSCSI réalisée et le volume monté, j'ai vérifié le bon fonctionnement en exécutant la commande « df » (pour Disk Free) sur chaque serveur de diffusion. Cette commande affiche des statistiques sur le taux d'occupation des disques. Pour chaque serveur, j'ai pu vérifier que la liaison avec le volume distant partagé en iSCSI était opérationnelle et correctement prise en compte.

L'installation du serveur RED5 a été réalisée à partir de l'archive proposée au téléchargement sur le site web de la solution. Le fichier obtenu est à décompresser dans un répertoire et contient tout les éléments nécessaires à la diffusion d'un flux en streaming. **Pour améliorer l'intégration du serveur de diffusion**, j'ai développé un script qui permet de démarrer et stopper la solution en même temps que le système hôte. De plus, **pour renforcer la sécurité**, j'ai mis en place une configuration qui cloisonne l'exécution du serveur de diffusion sous l'identité d'un compte d'utilisateur spécifique et non sous le compte de l'administrateur du système (compte root). Les actions et le script réalisés dans le cadre de cette étape sont fournis dans l'annexe IV de ce mémoire.

Dans le mode de configuration initial du serveur, les vidéos à diffuser en streaming doivent être copiées dans un sous-répertoire de la racine du serveur. Pour permettre la diffusion des vidéos stockées sur le serveur NAS distant, j'ai procédé à une redirection en détruisant le répertoire initial et en créant à la place un lien symbolique<sup>20</sup> vers le volume distant fournis par la couche de stockage partagé. Ainsi, chaque serveur de streaming peut accéder et diffuser les mêmes vidéos sans devoir en héberger une copie sur son système de fichier local. Nous verrons plus bas dans ce chapitre que ce mécanisme m'a été utile lors de la phase de test.

La **couche de répartition de charge** a été déployée en créant un nouveau serveur lui aussi virtualisé et installé avec une distribution Linux Debian. J'ai pris soin de faire exécuter ce serveur virtuel dans **un hyperviseur qui n'était pas déjà sollicité par un autre élément** de la solution afin de conserver l'indépendance physique entre équipement. Le serveur utilisé pour répartir la charge fait office de **serveur frontal** qui intercepte toutes les requêtes de consultation de flux multimédia. La charge de travail effective est ensuite **redirigée** vers l'un des serveurs de diffusion installés précédemment.

Le système de répartition de charge HaProxy a été installé en utilisant le gestionnaire de paquets de la distribution Debian. Le paramétrage de la répartition s'effectue à partir d'un unique fichier de configuration. L'esprit général du réglage à réaliser consiste à indiquer le port réseau que le serveur

---

<sup>20</sup> Un lien symbolique est une entrée spéciale dans les systèmes de fichier Unix qui permet de référencer de manière transparente d'autres entrées de répertoires ou de fichiers. On peut dire qu'un lien symbolique est un alias vers un autre fichier ou répertoire.

frontal doit écouter ainsi que les serveurs de diffusion vers lesquels les requêtes doivent être redirigées. Haproxy a également été configuré pour **interroger à intervalles réguliers** l'état de fonctionnement des serveurs qui lui sont rattachés. L'interrogation porte sur l'ouverture réussie d'une connexion réseau sur le port de diffusion des flux en streaming (Le port 1935 dans le cas du protocole RTMP). Ce mécanisme permet de détecter si un serveur de diffusion est indisponible et, le cas échéant, de ne plus lui transmettre de requêtes à traiter. Pour optimiser la répartition, il est également possible de choisir un algorithme d'équilibrage de charge particulier ou d'affecter un poids à chaque serveur de diffusion en fonction de ces capacités internes.

L'ensemble des informations et configurations traitées par HaProxy sont accessibles au travers d'une page web d'administration et de statistiques dont un exemple est fourni avec l'illustration n°32.

**HAProxy**  
**Statistics Report for pid 2692**

> **General process information**

pid = 2692 (process #1, nbproc = 1)  
 uptime = 91d 19h48m01s  
 system limits : memmax = unlimited ; ulimit-n = 8206  
 maxsock = 8206  
 maxconn = 4096 (current conns = 1)

active UP  
 active UP, going down  
 active DOWN, going up  
 active or backup DOWN

backup UP  
 backup UP, going down  
 backup DOWN, going up  
 not checked

Note: UP with load-balancing disabled is reported as "NOLB".

Display option:  
 • Hide DOWN servers  
 • Disable refresh  
 • Refresh now  
 • CSV export

External resources:  
 • Primary site  
 • Updates (v1.3)  
 • Online manual

RED5																								
Queue	Sessions					Bytes		Denied		Errors			Warnings			Server								
	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Conn	Resp	Retr	Redis	Status	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle	
svstream01	0	0	-	0	1	90	3	3	9084	10890	0	0	0	0	0	3d25m	UP	1	Y	-	71	1	30s	-
svstream02	0	0	-	0	1	90	2	2	4128	4273	0	0	0	0	0	3d19m	UP	1	Y	-	2	1	30s	-
Backend	0	0		0	2	0	5	5	13212	15163	0	0	0	0	0	91d19h	UP	2	2	0	0	0	0s	

CLIENTS																								
Queue	Sessions					Bytes		Denied		Errors			Warnings			Server								
	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Conn	Resp	Retr	Redis	Status	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle	
Frontend				0	2	2000	5		13212	15163	0	0	0			OPEN								

STATS																								
Queue	Sessions					Bytes		Denied		Errors			Warnings			Server								
	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Conn	Resp	Retr	Redis	Status	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle	
Frontend				1	1	2000	15		6443	56075	0	0	0			OPEN								

Illustration 32: Page web de statistiques du programme HaProxy

Cette page web est utile pour obtenir à distance un aperçu de l'état général du service de répartition de charge. Je l'ai utilisée de nombreuses fois pour vérifier le bon fonctionnement du système et obtenir des informations sur l'état des serveurs de diffusion rattachés. Des informations complémentaires relatives aux opérations que j'ai réalisées dans le cadre du déploiement et de la configuration du logiciel HaProxy sont fournis au sein de l'annexe V de ce mémoire.

La **couche d'accès client** a été réalisée **en développant une page web spécifique** permettant d'afficher dans un navigateur un lecteur multimédia compatible avec les flux en streaming. Le lecteur multimédia sélectionné se nomme « FLV Player » (<http://flv-player.net>). Il s'agit d'un programme Flash compilé qui s'exécute dans une page web après avoir été inséré à l'aide de la balise OBJECT<sup>21</sup> du langage HTML. L'intégration du lecteur dans la page web n'est pas suffisante pour démarrer la consultation d'une vidéo. Des paramètres supplémentaires doivent être ajoutés à la balise pour spécifier l'adresse du serveur frontal de répartition de charge et le nom du fichier à visionner. L'inconvénient de cette approche est qu'elle contraint à une utilisation statique de la page web car les caractéristiques de la vidéo à consulter sont figés dans son code. Pour remédier à cette limitation, **j'ai développé un mécanisme** qui permet de **spécifier la vidéo à consulter dans l'URL d'appel de la page**. Le code ci-dessous donne un aperçu du style d'écriture des URL à utiliser :

21 La balise OBJECT du langage HTML offre une solution générale pour l'inclusion d'objets génériques. La balise permet de spécifier les éléments nécessaires à la présentation de l'objet référencé tels le code source, les valeurs initiales et les données d'exécution.

`http://<nom du serveur>/<nom de la page web>?flv=<nom du fichier du média>`

<nom du serveur> désigne le serveur frontal de répartition de charge,  
<nom de la page web> désigne le nom de fichier de la page web développée,  
<nom du fichier du média> désigne le nom de fichier de la vidéo à visualiser.

Un code JavaScript que j'ai également développé prend alors en charge l'analyse de l'URL, extrait le nom du fichier du média et **affecte en dynamique** les paramètres du lecteur multimédia pour qu'il affiche la bonne vidéo. Grâce à ce dispositif, je n'ai eu à réaliser qu'une seule page web **pour rendre possible la consultation d'un nombre illimité de médias**. De plus, les compétences nécessaires à la création des URL ne nécessitant pas de connaissance en programmation, il devient possible d'intégrer aisément des liens vers un média à consulter en streaming dans une ressource pédagogique. Des précisions supplémentaires et le listing des codes développés pour ce système sont fournis en annexe VI de ce mémoire.

Enfin, ma réalisation a porté sur la **transmission des éléments de connaissance** nécessaires à la création de liens pointant vers une ressource multimédia diffusée en streaming au sein des ressources pédagogiques. Pour cela, j'ai rencontré un membre du bureau enseignement numérique et simulation (BENS) dont les fonctions visent notamment à assurer une veille technologique relative aux techniques et logiciels qui évoluent dans le domaine de l'enseignement numérique. Je lui ai expliqué le mécanisme de création des URL présenté précédemment afin qu'il soit capable de les intégrer dans le contenu pédagogique déjà existant du service de cours en ligne.

#### **- Validation et test**

Les tests et la validation de la plate-forme de diffusion en streaming ont été réalisés **en plusieurs étapes et selon plusieurs niveaux**.

- J'ai d'abord procédé à **différents tests depuis ma station de travail** après que toutes les couches du modèle de fonctionnement de la plate-forme de diffusion aient été réalisées.

**Le fonctionnement de chaque serveur de diffusion a été testé individuellement** en utilisant le lecteur FLV Player configuré pour un accès direct à chaque serveur sans passer par la couche de répartition de charge. J'ai pu alors vérifier le rendu effectif d'une vidéo de test déposée sur le volume de stockage partagé. Je me suis également assuré de la possibilité d'effectuer des bons en avant ou en arrière durant la diffusion du média et de la prise en compte immédiate de la nouvelle position de lecture.

**Le fonctionnement du serveur frontal de répartition de charge a été testé** pour vérifier qu'il distribue correctement les tâches à chacun de ses serveurs de diffusion référencés. A cet effet, j'ai modifié **temporairement** le comportement des serveurs de diffusion afin qu'ils exploitent des vidéos stockées **en local** et non plus celles hébergées par la couche de stockage partagé. Pour cela, je n'ai eu qu'à modifier le lien symbolique présenté plus haut dans ce chapitre lors de la réalisation de la couche de diffusion et le faire pointer vers un répertoire local. J'ai placé ensuite sur chacun des serveurs de diffusion **une seule vidéo de test à chaque fois différente mais portant le même nom de fichier**. Sur mon poste de travail, j'ai alors utilisé deux navigateurs avec lesquels j'ai envoyé une requête de consultation au serveur frontal pour qu'il affiche la vidéo correspondant à ce nom de fichier. J'ai pu alors vérifier que malgré l'émission de deux requêtes portant sur le même fichier, **ce n'était pas la même vidéo qui s'affichait dans chaque navigateur**. Ce résultat m'a

permis de confirmer que le serveur frontal avait bien réparti la même requête de consultation auprès de deux serveurs de diffusion différents. Cette vérification visuelle a ensuite été validée définitivement en consultant les fichiers de journalisation du serveur de répartition.

- Après avoir validé le fonctionnement nominal de la plate-forme de diffusion j'ai procédé à des **tests de fluidité de diffusion en streaming en fonction de la distance de consultation**. Ces tests ont été réalisés à partir de 5 localisations différentes et ont porté sur un jeu d'essai de huit vidéos aux caractéristiques variées.

Les localisations de tests que j'ai choisi sont reportées par ordre de distance croissante vis-à-vis de l'École des transmissions dans la liste ci-dessous :

- Localisation dans les bâtiments de l'ETRS.  
La ligne Internet mise en jeu est une ligne haut débit garantie à 20 Mbits/sec<sup>22</sup>.
- Localisation depuis mon domicile, situé à environ 10 km de l'ETRS.  
La ligne Internet mise en jeu est une ligne ADSL dimensionnée à 512 Kbits/sec.
- Localisation chez un membre de ma famille situé près de Tours, à environ 200 km de l'ETRS. La ligne Internet mise en jeu est une ligne ADSL dimensionnée à 512 Kbits/sec.
- Localisation aux États-Unis, à New York, avec l'aide d'un ami résident.  
La ligne Internet mise en jeu est une ligne ADSL dimensionnée à 2 Mbits/sec.
- Localisation en Afghanistan sur un théâtre d'opération extérieure, avec l'aide d'un personnel de l'ETRS. La ligne Internet est une ligne Afghane dimensionnée à 128 Kbits/sec.

Étant présent lors des tests effectués depuis l'ETRS, mon domicile et celui du membre de ma famille, j'ai pu déployer le même script de test de montée en charge que celui utilisé lors de la phase d'étude et de conception associée au service de cours en ligne. Pour mémoire, ce script m'avait permis de **simuler auprès d'un serveur de diffusion plusieurs connexions consommatrices de flux en streaming** en adoptant le même comportement que celui d'un lecteur multimédia. L'intérêt de ce script réside ici dans sa capacité à me permettre de **vérifier que la solution répond bien à l'une des contraintes de l'expression de besoin** visant à s'assurer que la plate-forme résiste à la consultation simultanée de 200 vidéos. En revanche, en raison de la difficulté technique de mise en œuvre, je n'ai pas été en mesure de sous-traiter l'exécution de ce script aux personnes localisées aux États-Unis et sur le théâtre d'opération Afghan. Dans les faits, **je dispose donc d'un retour d'expérience sur la résistance à la montée en charge uniquement pour les trois premières localisations de ces tests**.

Les caractéristiques des vidéos du jeu d'essai sur lesquelles j'ai agis sont celles qui impactent la bande passante mise en jeu et la fluidité de la restitution. Il s'agit des caractéristiques de résolution, de mode phonique et du taux d'échantillonnage.

- La **résolution** définit la taille de la vidéo et s'exprime en pixel.  
Pour mes tests, j'ai choisi les deux résolutions désignées comme standard de fait dans le monde de la diffusion vidéo sur Internet (hors haute définition). Il s'agit du format 320x240 et 640x480.
- Le **mode phonique** exprime le nombre de piste audio à restituer. Le mode stéréophonique indique deux pistes et le mode monophonique une seule piste. Un son monophonique nécessite moins de données qu'un son stéréophonique pour être rendu.
- Le **taux d'échantillonnage** définit la quantité d'information nécessaire à la restitution d'une seconde de média. La qualité de restitution est dépendante du taux d'échantillonnage mais

---

22 Les caractéristiques de la ligne Internet de l'École des transmissions ont été présentées lors de l'étude de l'existant technique.

aussi de la résolution du média et de son mode phonique. Pour le même taux d'échantillonnage, une vidéo de grande résolution en stéréophonie sera moins bien rendue qu'une vidéo de petite résolution en monophonie. Les valeurs retenues pour le test sont de 256 Kbits/sec et 512 Kbits/sec. Là encore, il s'agit des standards de fait rencontrés par exemple sur les grands sites Internet de diffusion en streaming (hors haute définition) tels YouTube ou DailyMotion.

Pour chaque localisation, l'accès aux huit vidéos du jeu d'essai a été testé. L'ensemble des résultats obtenus est présenté au tableau n°10.

Localisation du client	Résultats des test
Interne à l'école	<p>La lecture d'une vidéo de test est <b>fluide</b> quels que soient la résolution, le mode phonique et le taux d'échantillonnage.</p> <p>Le même résultat est également obtenu avec 200 connexions simultanées.</p>
Depuis mon domicile. (distance : environ 10 km)	<p>La lecture d'une vidéo de test est <b>fluide</b> quels que soient la résolution, le mode phonique et le taux d'échantillonnage.</p> <p>Le même résultat est également obtenu avec 200 connexions simultanées.</p>
Chez un membre de ma famille (distance : environ 200 km)	<p>La lecture d'une vidéo de test est <b>fluide</b> quels que soient la résolution, le mode phonique et le taux d'échantillonnage.</p> <p>En charge avec 200 connexions simultanées, j'observe parfois un <b>ralentissement de quelques millisecondes</b> lors de la consultation de la vidéo de test de plus grande résolution et de meilleure qualité. Ce ralentissement est lié à la mise en cache de la vidéo dans le lecteur multimédia.</p>
Aux États-Unis, à New York (distance : environ 6 000 km)	<p>La lecture d'une vidéo de test est <b>fluide</b> quels que soient la résolution, le mode phonique et le taux d'échantillonnage.</p> <p><b>Le test de montée en charge n'a pas pu être effectué.</b></p>
Depuis un théâtre d'opération afghan. (distance : environ 5 500km)	<p>L'utilisateur constate une <b>lecture par tranche</b> de 10 secondes puis une mise en cache de 15 secondes même avec une vidéo de résolution 320x240 en mode monophonique et avec un taux d'échantillonnage de 256 Kbits/sec.</p>

Tableau 10: Synthèse des tests de la plate-forme de diffusion en streaming

En synthèse, les résultats des tests de la plate-forme de diffusion en streaming révèlent les points suivants :

**La consultation d'une vidéo en Afghanistan n'a pas aboutie.** La ligne Internet de 128 Kbits/sec utilisée ne permet pas une visualisation correcte de la vidéo car la lecture est saccadée à cause du temps de chargement du cache. Un test avec une vidéo encodée avec un taux d'échantillonnage de 128 Kbits/sec pourrait sembler être la solution. Je n'ai cependant pas procédé à cet essai car une vidéo présentant cette caractéristique est de si mauvaise qualité visuelle (tâches sur la vidéo, pixellisation excessive) que le confort pédagogique ne sera pas assuré.

Pour toutes les autres destinations, **la consultation de la vidéo de test de plus grande résolution et de meilleure qualité a été validée.** Pour la France, le test de montée en charge à 200 connexions simultanées donne un résultat positif. En fonction des caractéristiques de la vidéo, **des ralentissements de quelques millisecondes** ont toutefois été observés lors du test de montée en charge effectuée à 200 km de l'école.

### **- Conversion des vidéos**

Comme je l'ai annoncé lors de la phase de conception, les vidéos existantes du service de cours en ligne n'étaient pas compatibles en l'état avec la plate-forme de diffusion en streaming et une conversion préalable était nécessaire. Lors de la réalisation de la solution, je n'ai pu aborder cette conversion qu'après avoir effectué la phase de test présentée précédemment afin de disposer d'un retour d'expérience cohérent au sujet du fonctionnement et des performances du système. En regard des résultats obtenus, j'ai donc pu identifier quelques caractéristiques capables d'améliorer significativement la qualité de diffusion des vidéos en streaming.

Dans un premier temps, **j'ai choisi le mode audio monophonique.** En effet, bien qu'un rendu stéréophonique soit plus agréable à l'oreille, ce niveau de qualité sonore ne se justifie pas pour restituer la voix d'une personne qui parle durant une séance de cours filmé. La stéréophonie est donc écartée car le volume supplémentaire de données à traiter surchargerait inutilement la bande passante du réseau sans apporter de réelle plus-value pédagogique.

Ensuite, **j'ai choisi une résolution de 320x240 pixels** pour limiter encore plus les ressources nécessaires à la diffusion des médias. Ma décision a été influencée par les quelques ralentissements que j'ai pu observer lors de la visualisation d'une vidéo de résolution 640x480 effectuée à 200 km de l'École des transmissions. L'objectif ici est de permettre au plus grand nombre de stagiaires de pouvoir bénéficier de flux multimédias diffusés en streaming.

Enfin, **j'ai choisi un taux d'échantillonnage de 512 Kbits/sec** car cette valeur permet d'encoder des vidéos qui se révèlent fluides à la lecture et peuvent afficher à l'écran des scènes rapides en conservant un bon niveau de détails pour chaque image affichée.

La **conversion des vidéos existantes** du service de cours en ligne a été une tâche fastidieuse. Comme je l'ai annoncé lors de l'étude du besoin, le volume de vidéo concerné affichait une taille globale de 9 Go pour environ 430 fichiers. En soit la conversion d'une vidéo d'un format à l'autre n'est pas difficile mais **la gestion manuelle d'un tel volume de donnée peut s'avérer excessivement longue**, de l'ordre de plusieurs jours sur un poste de travail standard.

Pour remédier à cet inconvénient, j'ai choisi de **développer un script qui prenne en charge la phase de conversion des vidéos.** J'ai choisi d'exécuter ce script sur un système Linux et d'utiliser

le programme de conversion de média « ffmpeg » (<http://www.ffmpeg.org>) qui est une interface en mode console de la librairie libffmpeg. Cette librairie est à la base de tous les programmes multimédias du monde Linux tels les logiciels de visualisation de vidéo, d'écoute audio, de montage ou de conversion de média. Le script créé s'est appuyé sur une architecture simple. D'un coté, l'ensemble des fichiers vidéos originaux du service de cours en ligne étaient déposés dans un répertoire. Par un système de recherche en boucle fondée sur la commande « find », le script effectuait alors une conversion de chaque vidéo rencontrée dans un format compatible avec la diffusion en streaming Flash Vidéo. Le fichier obtenu était alors copié dans un second répertoire. En exécutant ce script sur un serveur virtualisé que j'ai temporairement doté de 4 processeurs virtuels et de 10 Go de mémoire vive, j'ai pu effectuer la conversion de **toutes les vidéos du service de cours en ligne en une seule nuit**.

Une fois opérationnelle, **la plate-forme de diffusion en streaming a été présentée officiellement au général commandant l'École des transmissions** lors du comité de pilotage du projet CAN organisé le 11 octobre 2010. A l'issue de cette présentation, le général a formulé des commentaires encourageants au sujet du travail réalisé et a demandé à ce que la plate-forme bascule en production.

### **- Amélioration continue et perspectives d'évolution**

L'architecture que j'ai réalisée autorise un processus d'amélioration continue réel grâce à la possibilité d'adjonction de serveurs de diffusion supplémentaires au sein de la couche de répartition de charge. Puisque chaque serveur de diffusion supporte une centaine de connexions simultanées, **une première amélioration pourrait consister à mettre en service un troisième serveur de diffusion**. Pour supporter la contrainte des 200 connexions simultanées formulée par l'expression de besoin, chacun des trois serveurs serait alors sollicité à hauteur d'environ 65% de ses capacités.

Le serveur RED5 est un projet open-source développé par une communauté active. Bien qu'il soit tout à fait opérationnel, il ne se positionne pas au même niveau de performance que les serveurs professionnels. Lors de la phase de conception de la solution, j'ai testé plusieurs plates-formes de diffusion en streaming. Si j'ai choisi le serveur RED5 pour ses bons résultats et sa gratuité, j'ai aussi identifié la solution Wowza Serveur (<http://www.wowzamedia.com>) lors de mes recherches. J'ai pu tester ce serveur durant 30 jours grâce à une licence de démonstration. Pour un coût d'environ 800 dollars par serveur, ce produit m'a semblé **plus robuste et présentait de meilleures performances que celles du serveur RED5**. Actuellement, cette solution est notamment utilisée dans des sites web institutionnels étrangers ou par des plates-formes de ventes en ligne.

Pour permettre la consultation de flux pédagogiques multimédias depuis l'Afghanistan ou tout autre zone qui présente une faible bande passante, **le service de cours en ligne pourrait proposer des ressources pédagogiques de type audio**. Ces ressources seraient toujours diffusées au format Flash mais seraient allégées de leur composante vidéo. Ainsi, une bande passante de 128 Kbits/sec, voire même 96 Kbits/sec, serait suffisante pour faire transiter du son monophonique en streaming. Les ressources à diffuser devraient être produites intégralement et conçues pour supporter ce modèle pédagogique. En effet, la seule extraction de la bande son d'une vidéo de cours filmé ne suffit pas à générer une ressource audio exploitable car les messages ainsi délivrés, privés de la composante visuelle initiale, n'ont plus le même sens ou sont incompréhensibles pour les stagiaires.

Enfin, je formule une dernière proposition d'amélioration relative à la procédure de test de montée en charge de la plate-forme. Dans sa forme actuelle, le script développé donne pleinement satisfaction et permet de simuler efficacement un nombre choisi de connexions simultanées. En



revanche, il existe une limitation dans le sens où je ne suis pas capable de **simuler plus finement le comportement des utilisateurs durant leur connexion**. Par exemple, il pourrait être intéressant d'imiter des utilisateurs qui consultent des médias en effectuant des sauts en avant ou en arrière durant la diffusion ou d'autres qui mettent régulièrement la lecture en pause. Pour simuler de tels comportements, il existe une extension nommée « selenium » (<http://seleniumhq.org/projects/ide>) qu'il faut ajouter au navigateur Firefox (<http://www.mozilla-europe.org/fr>). Cette extension permet d'enregistrer le comportement initial d'un utilisateur et de le répéter autant de fois que nécessaire pour effectuer des tests. Dans une utilisation plus poussée, cette extension permet également de programmer des interactions encore plus fines et de simuler plus précisément un comportement voulu. L'utilisation d'une telle fonctionnalité serait un plus **pour tester dans des conditions proches de la réalité** le comportement de la plate-forme de diffusion en streaming.

*Cette partie a permis de présenter la réalisation des solutions associées au service de cours en ligne. Elle s'est concrétisée par le déploiement d'une plate-forme de diffusion en streaming de flux multimédias.*

*Le modèle de fonctionnement global de la plate-forme imaginé lors de la phase de conception a été divisé en plusieurs couches. Ces couches ont servi de cadre d'exécution durant la réalisation et ont permis de guider et ordonnancer les tâches. On retrouve donc du côté des serveurs une partie en charge du stockage partagé des vidéos, une autre en charge de la diffusion en streaming et une dernière responsable de la répartition de charge.*

*Enfin, du côté des clients, un page web spécifique affichant un lecteur multimédia capable de gérer des médias diffusés en streaming a été développée. Un mécanisme supplémentaire permet de spécifier la vidéo à consulter directement dans l'URL d'appel de la page web et confère ainsi à l'ensemble un fonctionnement dynamique.*

## 6.4 : Synthèse

*Dans le but d'analyse la phase de réalisation, cette partie expose une synthèse des actions effectuées. Il s'agit d'établir un bilan général, de présenter le travail accompli et de commenter les résultats obtenus.*

La phase de réalisation des solutions rattachées au service d'accès et d'authentification et au service de cours en ligne est finalisée. L'ensemble des solutions déployées est présenté en synthèse dans le tableau ci-dessous :

Service d'accès et d'authentification	Service de cours en ligne
<ul style="list-style-type: none"> <li>- Déploiement d'une fonction de filtrage personnalisée quel que soit le système d'exploitation mis en œuvre,</li> <li>- Mise en œuvre d'un portail captif pour imposer la politique de sécurité entre la zone d'hébergement et la DMZ.</li> </ul>	<ul style="list-style-type: none"> <li>- Mise en œuvre d'un service de diffusion de flux multimédias en streaming. Architecture en briques indépendantes et système de répartition de charge entre serveurs de diffusion,</li> <li>- Développement d'une page web dynamique de consultation de ressources multimédias diffusées en streaming.</li> </ul>

*Tableau 11: Synthèse des solutions réalisées*

**Les éléments déployés répondent à l'expression du besoin** et mettent en œuvre une solution de diffusion des flux pédagogiques multimédias sur l'espace numérique de travail. **Les contraintes et**

**les exigences formulées sont respectées** et leur prise en compte a été validée dès la phase de test des solutions par le comité de pilotage du projet CAN.

La plate-forme de diffusion en streaming du service de cours en ligne est un élément central de la phase de réalisation et contribue à **améliorer le confort pédagogique des stagiaires**. Grâce à la diffusion en continue, le temps de chargement et de consultation d'un média n'est plus dépendant du volume de la ressource utilisée.

D'un point de vue technique, l'architecture de cette plate-forme a été conçue selon un modèle à quatre couches qui présentent des caractéristiques de fiabilité, de disponibilité et d'évolutivité élevées. Par exemple, grâce à la couche de répartition de charge entre serveurs de diffusion, la montée en puissance du service de cours en ligne est gérée sans devoir remettre en cause la totalité du système.

D'un point de vue fonctionnel, les travaux réalisés dans le cadre de la conception et du déploiement de la plate-forme ont permis de faire **évoluer l'état d'esprit des personnes en charge de la mise en œuvre de l'espace numérique de travail**. Par exemple, alors que l'accent a longtemps été porté sur la qualité d'enregistrement des médias, les tests de diffusion et le retour d'expérience ont mis en avant la nécessité de réduire la taille ou la définition des vidéos afin de garantir cette fois une bonne qualité de diffusion. Par ailleurs, l'amélioration des capacités de diffusion multimédias va inciter les concepteurs de ressources pédagogiques à enrichir leurs réalisations et, de fait, les rendre plus attractives pour l'utilisateur.

Enfin, les améliorations apportées au service d'accès et d'authentification ont **renforcées l'infrastructure informatiques**. Ces ressources sont essentielles au fonctionnement du système d'information de la formation et à l'espace numérique de travail.

*La phase de réalisation a permis de déployer des solutions répondant à l'expression de besoin initiale du projet. Les résultats des tests opérationnels et le retour d'expérience vont dans ce sens.*

*Au delà de l'aspect technique, le projet a contribué à renforcer les connaissances fonctionnelles rattachées au domaine de l'enseignement numérique et a dégagé de nouvelles possibilités pour la création de ressource pédagogique.*

---

*Ce chapitre a présenté la phase de réalisation des solutions que j'ai menée dans le cadre de mon projet CNAM.*

*Ma démarche s'est d'abord attachée à étudier et prendre en compte le contexte général de réalisation. A cet effet, j'ai présenté les contraintes et les difficultés auxquelles j'ai dû faire face durant mes actions.*

*Ensuite, dans la continuité de la démarche orientée service déjà utilisée lors de la phase de conception, j'ai réalisée les solutions destinées au service d'accès et d'authentification et au service de cours en ligne de l'espace numérique de travail.*

*Le résultat final fait état d'une réalisation opérationnelle qui répond bien aux contraintes et exigences formulées dans l'expression du besoin et visant à disposer d'une solution de diffusion des flux pédagogiques multimédias de l'espace numérique de travail.*

## 7 : CONCLUSION

L'enseignement numérique est manifestement une alternative crédible, voire un complément, vis-à-vis du mode de formation historique reposant sur le face à face pédagogique. Les avantages de cette discipline sont multiples comme par exemple délocaliser la formation, réduire les contraintes de lieux et de temps, absorber les flux de stagiaires imprévus ou adapter les flux de formation pour des besoins ponctuels et opérationnels. Sa mise en œuvre nécessite toutefois des investissements techniques et fonctionnels conséquents et impose de transformer les organisations en profondeur. A ce titre, un tel projet ne peut être réussi que s'il est accepté par l'ensemble de l'organisme de formation concerné et par les apprenants.

Depuis l'année 2008, l'École des transmissions du ministère de la défense mène une démarche d'appropriation et de mise en œuvre du mode de partage de la connaissance basé sur l'enseignement à distance et les communautés de pratiques professionnelles au travers du projet Campus Area Network (CAN). Les travaux qu'elle a réalisés lui ont progressivement permis de proposer à ses stagiaires et à l'ensemble du personnel du ministère de la défense un espace numérique de travail offrant des services à vocation pédagogique et collaborative. Le projet CAN est géré selon une approche orientée service et fait appel au recueil de bonnes pratiques ITIL. Par service, il faut entendre ici un ensemble d'éléments connexes fournis à l'appui d'un ou plusieurs processus métiers. L'intérêt de cette approche est qu'elle permet d'identifier et d'isoler les éléments d'un projet et de mettre en œuvre une politique de gestion personnalisée pour chacun d'entre eux. Pour cela, la structure de conduite du projet CAN repose sur un comité de pilotage qui valide les choix et les décisions relatifs à chaque service.

Le projet associé à ce mémoire s'intègre au projet CAN de l'École des transmissions au travers de son espace numérique de travail. Par extension, il a donc été piloté selon une approche orientée service ITIL et validé en comité de pilotage. Ce contexte d'exécution a positionné le projet à un niveau stratégique par le commandement de l'école. Il a permis de s'intégrer dans une structure de projet de grande envergure au sein d'une organisation complexe. Cette situation a imposé méthode et rigueur dans la réalisation des phases de conception, de transition et d'exploitation afin de les intégrer dans un existant opérationnel et maintenir la continuité des services.

L'expression de besoin formulée par le directeur du projet avait pour finalité de concevoir et réaliser une solution de diffusion des flux pédagogiques multimédias. Initialement, la consultation des ressources pédagogiques numériques était parfois saccadée et débutait après un temps de latence. Ce dysfonctionnement impactait alors directement le confort pédagogique des stagiaires et nuisait à l'adoption et au développement du mode de partage de la connaissance basé sur l'enseignement à distance.

Pour répondre à ce besoin, il a d'abord été nécessaire de mener une étude approfondie du domaine de l'enseignement numérique et d'évaluer le périmètre et l'intégration de ses composantes techniques, fonctionnelles et pédagogiques pour répondre au besoin d'une école militaire. Ensuite, la démarche générale retenue a consisté à identifier les services ITIL impactés par le projet : le service d'accès et d'authentification et le service de cours en ligne. L'une des solutions réalisées a permis de mettre en œuvre une plate-forme de diffusion continue de flux multimédias et d'améliorer la qualité de service de consultation des ressources pédagogiques. Cette solution a abouti sur la création d'un nouveau service de diffusion des contenus. L'architecture conçue pour cette réalisation repose sur un modèle en briques qui permet de s'adapter à la montée en charge. Chaque brique apporte une fonctionnalité identifiée à l'infrastructure.

Enfin, la capacité à pouvoir s'entraîner, simuler, acquérir des actes réflexes ou apprendre des techniques spécifiques est indispensable pour un stagiaire militaire, qu'il soit en métropole ou sur un théâtre d'opération. A ce titre, la capacité pour l'École des transmissions à pouvoir diffuser des connaissances en enseignement à distance est essentielle. De plus, cette transmission doit pouvoir intégrer une composante visuelle car ce mode est plus propice à l'acheminement de connaissances basées sur le geste, telles certaines techniques de combat ou de mise en œuvre de système d'information et de communication. Ce mémoire couvre à cet effet un besoin important en permettant à l'espace numérique de travail de diffuser en continu et sans interruption des flux multimédias au sein des ressources pédagogiques numériques. Les perspectives d'évolution sont nombreuses et autorisent par exemple d'envisager la transmission de connaissance en utilisant des supports mobiles du commerce comme les téléphones ou les tablettes tactiles ou d'exploiter la représentation en trois dimensions en acheminant les données en streaming.

A titre personnel, ce mémoire marque pour moi l'achèvement d'un parcours de formation d'ingénieur qui a profondément marqué ces quatre dernières années. Hormis le renforcement indéniable de mes compétences techniques, je retiens de cette période une évolution notable de mon état d'esprit et l'appropriation au fil du temps d'une nouvelle mentalité. Durant ma formation, j'ai en effet dépassé le périmètre de technicien expérimenté et me suis progressivement positionné à un niveau plus élevé tant sur le plan de la réflexion que celui de l'action. J'ai acquis des techniques qui me permettent de mieux appréhender les risques d'un projet et, de ce fait, d'aborder des problèmes d'envergure. J'ai pris goût à développer des raisonnements rigoureux et justifiés qui servent la stratégie globale de l'entreprise et non plus seulement les intérêts d'un service. Si le caractère, l'expérience et la compétence participent activement à une telle mutation, seul le sentiment de légitimité permet de mener la transformation à terme et de la maintenir dans le temps. Cette légitimité, je considère que c'est ma formation d'ingénieur CNAM qui me l'a donnée. Mes objectifs pour les années à venir consistent donc à maintenir et développer ma légitimité d'ingénieur. J'envisage pour cela de mettre en pratique les connaissances que j'ai reçues durant ma formation mais aussi de les transmettre autour de moi. A moyen terme, je souhaite pouvoir continuer à évoluer professionnellement et à me positionner sur des postes qui intègrent bien cette nouvelle dimension.

# ANNEXE 1 : PORTEFEUILLE DES SERVICES DE L'ENT

Version 1.3 du portefeuille de services au 18/08/2010.

N°	Service	Client	Propriétaire	Date de maquette	Date de production	Au catalogue Internet/Intraterre	Détail de la version
1	Accès et authentification	F/S/A	BFAO	01/01/09 31/03/09 20/03/10 01/04/10 15/06/10	31/03/09 01/11/09 01/10/10 15/12/10 01/07/10	OUI/NON OUI/NON NON/NON NON/NON OUI/NON	Zone hébergement + interne Zone externe + PFI Portail captif zone hébergement Fédération identité IDP Accès portail par téléphone mobile
2	Messagerie	F/S	BFAO	01/10/09	01/07/10	OUI/NON	Webmail
3	Agenda partagé	F	BFAO	01/10/09	01/07/10	OUI/NON	Application horde
4	Emploi du temps en ligne	F/S	BFAO	01/01/10	01/07/10	OUI/OUI	Réplication SAGAIE EDT
5	Cours en ligne	F/S/A	BENS	01/01/09 01/10/09	31/03/09	OUI/OUI OUI/NON	Cours filmés + CISCO + Microsoft EAD parcours de formation LMS
6	Référencement ressources SIC	F/S/A	CRSICAT	01/10/09	15/07/20	OUI/OUI	Recherche ressources SIC
7	Ticket incident	F/S/A	BFAO	10/03/10	01/07/10	OUI/OUI	Helpdesk en ligne
8	TV en ligne en zone hébergement	S	BFAO	01/01/09	31/03/09	OUI/NON	300 chambres de la zone hébergement
9	Forum professionnel SIC	F/S/A	BENS	01/12/09	31/01/10	OUI/NON	Forum thématique SIC avec modérateur
10	Forum ETRS	F	BENS			NON/NON	Sur Intraterre, avec identification
11	Espace de stockage utilisateurs	F/S	BFAO	01/10/10	01/01/11	NON/NON	Serveur de fichiers
12	Liste de diffusion	F/S	BFAO	01/10/09	01/07/10	OUI/NON	Par messagerie (système SYMPA)
13	Annuaire	F/S/A	BFAO	01/03/10	01/07/10	OUI/NON	Interface Web
14	Chaîne éditoriale	F	BENS	01/08/10	01/01/11	NON/NON	Outil de publication
15	Générateur de QCM	F	BENS	01/09/10	01/01/11	NON/NON	Outil de questionnaire

Tableau 12: Portefeuille des services de l'espace numérique de travail

## **Légende :**

F = Formateurs et permanents ETRS – S = Stagiaires présents – A = Abonnés (personnel Défense hors F et S)

## ANNEXE 2 : ITIL VERSION 3

Information Technology Infrastructure Library (ITIL) est un ensemble d'ouvrages recensant les bonnes pratiques de gestion des services informatiques édités par l'office public britannique du commerce. Les sujets abordés traitent de l'organisation des systèmes d'information, de la façon d'améliorer leur efficacité, de la réduction des risques ou de la qualité.

La démarche ITIL repose sur une approche orientée processus qui accompagne la stratégie, la conception, la transition et l'exploitation des services et permet d'améliorer la qualité dans un contexte d'amélioration continue. Une modélisation synthétique de la méthode ITIL peut être représentée par l'illustration ci-dessous.

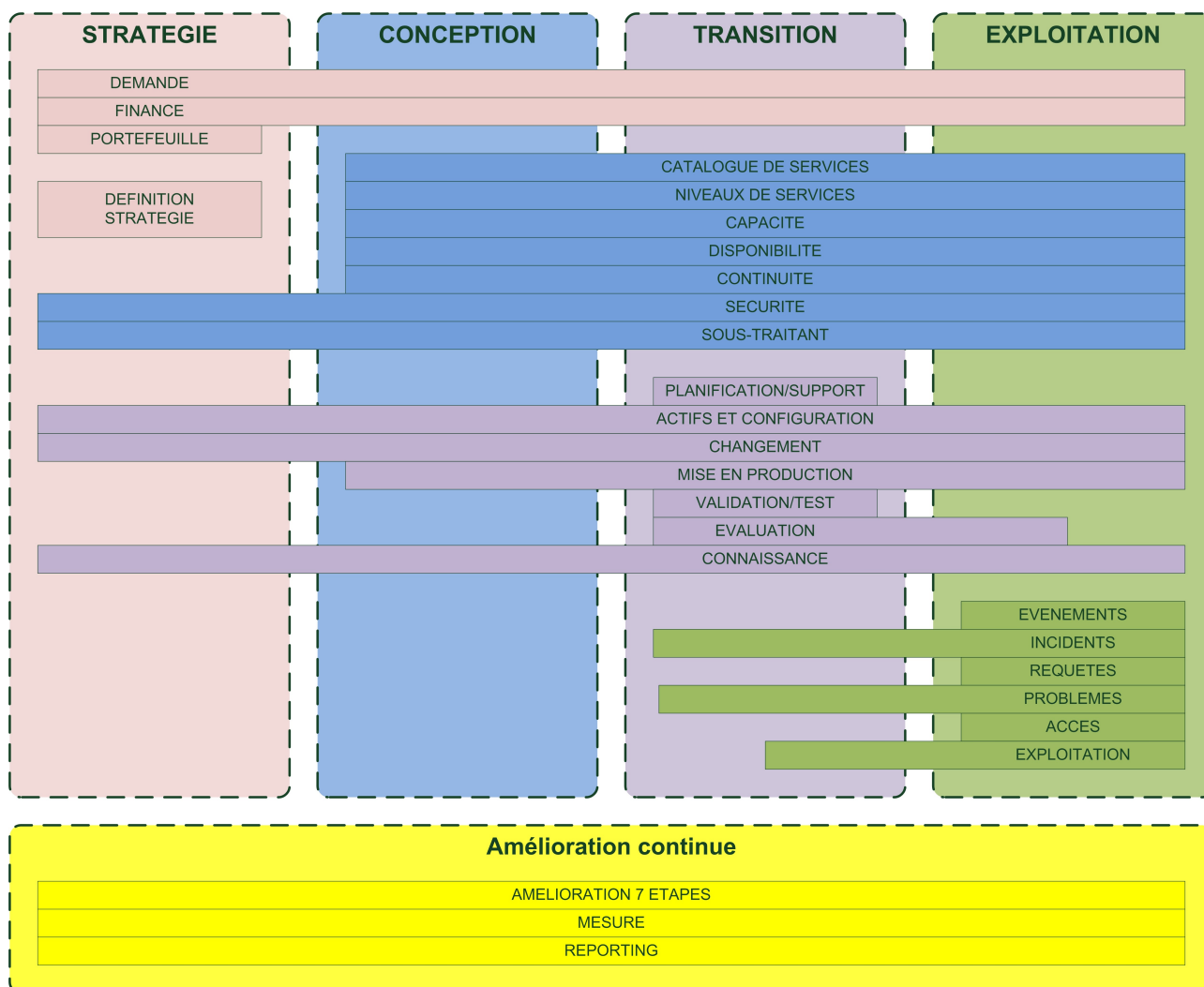


Illustration 33: Principes du recueil de bonnes pratiques ITIL v3

La gestion de la stratégie, de la conception, de la transition, de l'exploitation et de l'amélioration continue se décompose en sous-processus qui traitent de problématiques spécifiques. Un sous-processus initié dans une phase donnée peut continuer à s'exécuter au sein d'une ou de plusieurs phases suivantes. C'est la cas par exemple du sous-processus de gestion de la sécurité qui est initié pendant la phase de conception et reste actif lors de la phase de transition et d'exploitation du service.

ITIL n'est pas une méthodologie de conduite de projet mais permet d'accompagner les équipes en charge du pilotage lors de la planification et la coordination des opérations. Il convient donc de prendre du recul sur l'ensemble des préconisations formulées et d'être à même de les interpréter et de les adapter au contexte de réalisation de chaque projet.

La stratégie d'un service informatique a pour mission de le valoriser en définissant son utilité et en donnant une garantie de moyens d'une exécution conforme à la demande en termes de niveaux de disponibilité, capacité, continuité et sécurité.

La conception des services a pour objectif de convertir les objectifs stratégiques en des services disponibles au sein d'un portefeuille de services qui reflètent la stratégie du système d'information.

La transition des services permet de s'assurer que la mise en œuvre d'un nouveau service ou d'un service modifié s'effectue sans discontinuité dans l'exécution du système d'information conteneur.

L'exploitation des services est la partie du cycle de vie où les services et la valeur ajoutée sont effectivement livrés. Le suivi des problèmes ainsi que l'équilibre entre la fiabilité du service et le coût y sont pris en compte.

L'amélioration continue des services est un objectif transverse qui vise à augmenter la qualité grâce à la mise en place de systèmes de suivi et de reporting qui permettent de déceler les axes d'amélioration et de corriger les services en exécution.

## ANNEXE 3 : FONCTION DE FILTRAGE LOCALISÉE

La fonction de filtrage de chacun des serveurs équipés d'une distribution Linux repose sur le système « iptables ». Ce système puissant est natif au noyau Linux et un script shell chargé au démarrage du système suffit à le paramétrer.

L'inconvénient de ce type de solution est qu'il est nécessaire de déployer autant de scripts qu'il y a de serveurs à gérer et de personnaliser chaque script pour qu'il laisse passer les flux autorisés ou bloque les flux interdits en fonction de chaque serveur.

Pour pallier à cet inconvénient, j'ai procédé à l'installation du système « Puppet » qui permet de centraliser en un point unique sur un serveur dédié l'ensemble des scripts de configuration à déployer sur des serveurs clients. Puppet ne fait que copier les fichiers sur les clients. Le concepteur doit prendre en charge le contenu des configurations

Les serveurs qui doivent être gérés par le système doivent exécuter le client Puppet, un simple programme qui interroge à intervalles réguliers le serveur pour déterminer si une configuration doit être modifiée.

L'installation du serveur Puppet s'effectue grâce à la commande :

```
# aptitude install puppet-server
```

L'installation du client Puppet s'effectue grâce à la commande :

```
# aptitude install puppet
```

La configuration du serveur Puppet nécessite de paramétrer un fichier contenant la description des clients à gérer et des configurations qu'ils doivent importer. L'utilisation et le paramétrage plus avancés de Puppet dépasse le périmètre de cette annexe et ne seront pas plus détaillés.

Le système que j'ai développé permet de déployer sur chaque serveur client un script principal de configuration de firewall et plusieurs scripts secondaires. Les scripts secondaires permettent d'activer ou non des protocoles courants comme le HTTP, HTTPS, FTP, etc. Le script principal exécute sa configuration et scrute un second répertoire nommé « scripts-enabled » dans lequel se situent les scripts secondaires. Ainsi, la configuration personnalisée de chaque serveur est centralisée sur le serveur Puppet.

Ci-dessous, le script de firewall global exécuté sur chaque serveur :

```
#!/bin/bash
#
# Configuration de netfilter
#
#####
# Forcer le passage dans le répertoire du script
#####
if [ -L $0 ]
then
    scriptpath=`dirname $(readlink $0)`
else
    scriptpath=`dirname $0`
fi
```



```

cd $scriptpath

#####
# Configuration générique
#####

# Vider les règles existantes
iptables -F
iptables -X

# Rejeter tout le trafic par défaut
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Accepter le loopback
iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT

# Accepter les ping
iptables -A INPUT -p ICMP --icmp-type echo-request -m limit --limit 5/s --limit-burst 5 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type echo-reply -m limit --limit 5/s --limit-burst 5 -j ACCEPT

# Autoriser les connexions de la machine locale vers l'extérieur
iptables -A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

# Autoriser la réception de connexions initiées localement
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#####
# Configuration propre à la machine
#####
for file in ./scripts-enabled/*
do
    . $file
done

#####
# Configuration par défaut
#####

# Rejeter toutes les autres demandes de connexions provenant de l'extérieur
iptables -A INPUT -m state --state NEW -j REJECT

```

Ci-dessous, quelques exemples de scripts secondaires permettant la personnalisation des configurations :

```

# Autoriser les connexions LDAP
iptables -A INPUT -m state --state NEW -p TCP --sport 1024: --dport 389 -j ACCEPT

# Autoriser les connexions de type "web"
iptables -A INPUT -m state --state NEW -p TCP --sport 1024: --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -p TCP --sport 1024: --dport 443 -j ACCEPT

# Autoriser les connexions SSH
iptables -A INPUT -m state --state NEW -p TCP --sport 1024: --dport 3306 -j ACCEPT

```

## ANNEXE 4 : SERVEUR DE STREAMING RED5

L'accès en streaming à un flux multimédia nécessite la mise en œuvre de serveurs spécialisés capables de prendre en charge un protocole de diffusion continue. Le protocole de diffusion continue utilisé pour ajouter au service de cours en ligne la capacité à exploiter le streaming se nomme « Real Time Messaging Protocol » ou RTMP. Ce protocole a initialement été élaboré par la société Adobe pour sa technologie Flash. La solution déployée pour mettre en œuvre les serveurs RTMP du service de cours en ligne repose sur l'utilisation du logiciel libre RED5.

**Cette annexe décrit la procédure que j'ai développée afin de réaliser l'installation d'un serveur RED5 sur une machine Linux Debian.**

Au préalable des actions recensées ci-dessous, il est nécessaire d'être connecté sous le compte « root » d'une machine Linux équipée d'une distribution Debian Lenny (version 5).

Télécharger l'archive du serveur :

```
# mkdir /root/tmp && cd /root/tmp
# wget http://www.red5.org/downloads/0_8/red5-0.8.0.tar.gz
```

Décompresser le fichier package :

```
# mkdir /usr/local/red5
# tar -xzf red5-0.8.0.tar.gz -C /usr/local/red5
```

Rendre le fichiers « .bat » non exécutables.

```
# cd /usr/local/red5
# find . -type f -name "*.bat" | xargs chmod a-x
```

Créer un groupe et un utilisateur dédiés :

```
# addgroup --system red5
# adduser --system --shell /bin/sh --home /usr/local/red5 --ingroup red5 red5
# chown -R red5:red5 /usr/local/red5
```

Paramétrer les performances :

```
# su - red5 -c "./red5-highperf.sh"
```

Créer le script de démarrage et d'arrêt automatique du serveur (/etc/init.d/red5) et coller le contenu ci-dessous :

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          red5
# Required-Start:    $remote_fs $syslog
# Required-Stop:     $remote_fs $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Serveur red5
# Description:       Serveur de streaming red5.
### END INIT INFO

RED5_HOME="/usr/local/red5"
RED5_USER="red5"
SCRIPT_NAME="red5"

# Démarrer le serveur
do_start() {
```

```

    su -l $RED5_USER -c "$RED5_HOME/red5.sh &"

    return 0
}
# Arrêter le serveur
do_stop() {

    su -l $RED5_USER -c "$RED5_HOME/red5-shutdown.sh"

    return 0
}
case "$1" in

    start)
        do_start
        ;;

    stop)
        do_stop
        ;;

    *)
        echo "Usage : $SCRIPT_NAME {start|stop}"
        exit 1
        ;;

esac

```

#### Initialiser le script :

```

# chmod a+x /etc/init.d/red5
# update-rc.d red5 start 70 2 3 4 5 . stop 20 0 6 .

```

Dorénavant, le serveur démarre et s'arrête automatiquement en même temps que la machine hôte.

## ANNEXE 5 : RÉPARTITEUR DE CHARGE HAPROXY

HAProxy (<http://haproxy.1wt.eu>) désigne « High Availability proxy ». C'est un répartiteur de charge à haute disponibilité utilisé dans le cadre de ce projet pour mettre en œuvre la redondance entre les serveurs de streaming utilisés pour diffuser les flux multimédias du service de cours en ligne. Comme cela a été illustré dans les chapitres traitant de la conception et de la réalisation, HAProxy met en œuvre un serveur frontal et des serveurs enfants. Le frontal est placé en écoute des requêtes entrantes pour lequel il est configuré et sous-traite l'exécution réelle des demandes à l'un de ses serveurs enfants. Pour faire face à une augmentation de la charge, il suffit alors d'ajouter un serveur enfant et de le déclarer dans le serveur frontal. Les serveurs enfants ont pour unique client le serveur frontal. En revanche, ils ne nécessitent pas de configuration particulière et n'ont pas « conscience » d'être utilisés au sein d'un pool de serveurs.

HAProxy est présent dans la majorité des dépôts de paquetages des distributions Linux. Son installation a été réalisée grâce à la commande ci-dessous sur la plate-forme cible :

```
# aptitude install haproxy
```

La configuration du serveur frontal et la déclaration des serveurs enfants est à placer dans le fichier `/etc/haproxy/haproxy.cfg`. Son contenu est reflété par la configuration ci-dessous :

```
Global
    log 127.0.0.1        local0
    log 127.0.0.1        local1 notice
    maxconn 4096
    user haproxy
    group haproxy
    daemon

defaults
    log global
    option dontlognull
    timeout client 30s
    timeout server 30s
    timeout queue 30s
    timeout connect 4s
    retries 3
    stats enable
    stats refresh 5s
    stats uri /haproxy?stats
    stats hide-version

frontend STATS
    bind :8080
    mode http
    monitor-uri /haproxy?monitor

frontend CLIENTS
    bind :1935
    default_backend RED5

backend RED5
    mode tcp
    option httpchk
    balance roundrobin
    server svrstream01 X.X.X.X:1935 check port 5080 inter 15000 maxconn
```

90

```
server svrstream02 X.X.X.X:1935 check port 5080 inter 15000 maxconn
```

90

Pour les besoins de la solution déployée, HAProxy a été configuré selon les règles et contraintes ci-dessous :

- Le service HAProxy s'exécute sous un compte utilisateur dédié afin d'assurer le cloisonnement des processus avec le reste du système,
- Le serveur frontal vérifie toutes les 5 secondes l'état des serveurs enfants en effectuant une requête de test sur le port réseau dédié au transfert des données de streaming,
- Chaque serveur enfant est configuré pour accepter un maximum de 90 connexions simultanées. Au delà, le serveur frontal bloque les requêtes entrantes si tous les serveurs enfants ont atteint cette limite,
- Le serveur frontal assure le suivi de requête afin qu'une transaction avec un client soit toujours assurée par le même serveur enfant. Cette configuration est indispensable pour permettre, par exemple, le suivi de session HTTP et la mise en cache efficace des flux de lecture multimédia,
- L'algorithme de répartition de charge entre les serveurs enfants a été configuré pour être de type « roundrobin ». Cet algorithme réalise la répartition de charge en sollicitant les serveurs enfants de manière séquentielle. Il est possible d'attribuer un poids différents à chaque enfant afin qu'il participe de manière personnalisée à la répartition de la charge. Cette caractéristique offre une grande souplesse puisqu'elle permet d'utiliser des machines de puissance variable pour constituer le pool d'enfants.

## ANNEXE 6 : CONSULTATION EN STREAMING

La consultation d'une ressource en diffusion continue nécessite l'utilisation d'un programme client compatible avec le protocole mis en œuvre par le serveur de streaming. La solution déployée au profit du service de cours en ligne s'appuie sur le protocole « Real Time Messaging Protocol » (RTMP) et exploite des médias au format Flash Vidéo. Pour faciliter l'intégration de la solution au sein de l'existant, j'ai développé une page web spécifique qui affiche un lecteur multimédia compatible avec le protocole RTMP. Ce lecteur se nomme « FLV Player ». Il s'agit d'une application libre développée en langage Flash qui prend en charge la gestion des connexions au serveur et le traitement des flux en streaming. Ce lecteur peut s'intégrer dans une page web en utilisant la balise « <object> » du langage HTML. En l'état, ce mode de fonctionnement présente un problème de flexibilité car l'intégration du lecteur dans la page nécessite de coder en dur le nom de la ressource qu'il doit afficher. En mode statique, il faut donc développer autant de pages web qu'il y a de médias à visualiser.

Pour pallier à ce problème, j'ai développé une page web spécifique qui permet de spécifier le média que l'on veut visualiser directement dans l'URL de la page. Un code JavaScript permet ensuite d'analyser cette URL et d'intégrer en dynamique dans la page web le lecteur multimédia affecté des bons paramètres pour visualiser le média donné. Le formalisme de l'URL correspond au modèle ci-dessous :

```
http://<nom du serveur>/<nom de la page web>?flv=<nom du fichier du média>
```

Par exemple, si la page web est enregistrée dans le fichier « lecteur.html », qu'elle est stockée sur le serveur « svrstreaming » et que l'on souhaite visualiser en streaming la vidéo « exemple.flv », il faut appeler cette page avec l'URL :

```
http://svrstreaming/player.html?flv=exemple.flv
```

Sur appel de cette URL, la page web s'affichera dans le navigateur avec le lecteur multimédia paramétré pour diffuser en streaming la vidéo « exemple.flv ».

Grâce à ce mécanisme, il est possible de visualiser n'importe laquelle des vidéos du service de cours en ligne **sans coder de page web spécifique** et en utilisant uniquement un **mécanisme simple de construction des URL**.

Ci-dessous, le code de la page web développée. Le fichier qui contient le lecteur multimédia et le code JavaScript de gestion des URL doivent être situés dans un répertoire enfant nommé « js ». Le fichier de la bibliothèque « JQuery » que j'utilise pour l'analyse de bas niveau des URL doit également être présent dans ce répertoire :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" lang="fr">
<head>
    <title>Lecteur multimédia ETRS</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <script type="text/javascript" src="./js/jquery-1.4.2.min.js"></script>
    <script type="text/javascript" src="./js/jquery.swfobject.1-1-
1.min.js"></script>
    <script type="text/javascript" src="./js/script.js"></script>
</head>
<body>
<div id="flash">
```

```
<p>Vous lisez ce message car la page web ne peut pas afficher de
vidéo.</p>
<p><br/>Vérifiez le formatage de l'URL utilisée.</p>
<p>Vous devez installer le plugin Adobe Flash pour visualiser la
ressource.</p>
</div>
</body>
</html>
```

Ci-dessous, le code JavaScript qui prend en charge l'analyse des URL et le code d'intégration du lecteur multimédia affecté des paramètres permettant la visualisation de la vidéo souhaitée.

```
$(function()
{
    // Initialiser la récupération des paramètres de l'URL
    $.urlParam = function(name)
    {
        var results = new RegExp('[\\?&]' + name +
            '=[^&#]*').exec(window.location.href);

        if(results == null) return 0;
        return results[1] || 0;
    };

    // Instancier et positionner le lecteur multimédia
    var oflash = $("#flash");

    // Récupérer les paramètres
    var width = $.urlParam('width');
    if(width == 0) width = 320;
    var height = $.urlParam('height');
    if(height == 0) height = 280;

    oflash.flash(
    {   swf: './resources/player_flv_maxi.swf',
        play: true,
        width: width,
        height: height,
        flashvars: {
            title: "Ecole des Transmissions",
            flv: $.urlParam('flv'),
            showstop: '1',
            showvolume: '1',
            showtime: '2',
            netconnection: 'rtmp://stream.ent-etrns.net/oflaDemo',
            autoplay: '1'
        }
    });
});
```

## SIGLES ET ABRÉVIATIONS

<b>Sigle, abréviation</b>	<b>Description</b>
BENS	Bureau enseignement numérique et simulation
BFAO	Bureau de formation assistée par ordinateur
CAN	Campus area network
CAS	Central authentication service
CDROM	Compact disk – read only memory
CIRM	Centre informatique de ressources multimédias
CNAM	Conservatoire national des arts et métiers
CNED	Centre national d'éducation à distance
COMETRS	Commandant de l'école des transmissions
CRSICAT	Centre de ressources SIC de l'armée de terre
DEP	Directeur des études et de la prospective
DGF	Direction générale de la formation
DGSIC	Direction générale des systèmes d'information et de communication
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information
DMZ	Zone démilitarisée
DNS	Domain name service
DRHAT	Direction des ressources humaines de l'armée de terre
EAD	Enseignement à distance
EAO	Enseignement assisté par ordinateur
ENT	Espace numérique de travail
ETRS	École des transmissions
GT IA EAD	Groupe de travail interarmées de l'enseignement à distance
HTML	Hypertext markup language
HTTP	Hypertext transfert protocol
HTTPS	Hypertext transfert protocol secured
IPSec	Internet protocol security
ISCSI	Internet small computer system interface
ITIL	Information technology infrastructure library
LAN	Local area network



LDAP	Lightweight directory access protocol
LMS	Learning management system
MSIR	Module « systèmes informatiques et réseau »
NAS	Network attached storage
PFI	Plateforme d'instruction
QCM	Questionnaire à choix multiples
QoS	Quality of service
RTMP	Real time messaging protocol
SCSI	Small computer system interface
SDFE	Sous-direction de la formation et des écoles
SIC	Système d'information et de communication
SIF	Système d'information de la formation
SLA	Service level agreement
SSO	Single sign-on
TICE	Technologies de l'information et de communication pour l'éducation
URL	Uniform resource locator
VLAN	Virtual local area network
WAN	Wide area network
WIFI	Wireless fidelity

# INDEX DES ILLUSTRATIONS

Illustration 1: Structure organisationnelle de l'ETRS.....	8
Illustration 2: Planification du projet CAN depuis son lancement.....	10
Illustration 3: Planification du projet CNAM.....	11
Illustration 4: Organisation de l'enseignement dans l'armée de Terre.....	18
Illustration 5: Structure du GT IA EAD.....	19
Illustration 6: Évolution du nombre de stagiaires en mode présentiel par année scolaire.....	21
Illustration 7: Évolution du nombre d'auditeurs abonnés au module MSIR par année.....	23
Illustration 8: Modèle de fonctionnement du système d'information de la formation.....	28
Illustration 9: Schéma de principe du réseau d'enseignement global.....	32
Illustration 10: Schéma de principe de l'architecture Internet.....	33
Illustration 11: Situation géographique du système d'information de la formation.....	35
Illustration 12: Type de média selon l'approche document.....	42
Illustration 13: Type de média selon l'approche serveur.....	43
Illustration 14: Graphique de répartition des tailles de fichier vidéo.....	46
Illustration 15: Évolution moyenne du temps de latence avant accès à une vidéo.....	47
Illustration 16: Découpage en zones élémentaires du réseau d'enseignement connecté à l'Internet.....	53
Illustration 17: Schéma de principe du double abonnement internet.....	59
Illustration 18: Installation d'un portail captif en coupure de réseau.....	62
Illustration 19: Mesures de débit sur la carte réseau interne et externe de l'équipement.....	64
Illustration 20: Mesure d'activité moyenne des processeurs de l'équipement.....	65
Illustration 21: Amélioration du service d'accès entre les PFI, les stations cadre et la DMZ.....	67
Illustration 22: Nouvelle liaison entre les serveurs et l'environnement.....	69
Illustration 23: Le principe du streaming de ressource audio ou vidéo.....	73
Illustration 24: Montée en charge des processeurs durant un test de connexions simultanées.....	76
Illustration 25: Architecture générale de la solution de diffusion des vidéos Flash en streaming.....	77
Illustration 26: Planning de réalisation de la fonction de filtrage.....	81
Illustration 27: Principe de fonctionnement de la fonction de filtrage pour système Linux.....	82
Illustration 28: Planning de réalisation du portail captif.....	84
Illustration 29: Plate-forme de test pour l'installation du portail captif.....	85
Illustration 30: Planning de réalisation de la plate-forme de diffusion en streaming.....	89
Illustration 31: Schéma de principe de la baie de serveurs virtualisés.....	90
Illustration 32: Page web de statistiques du programme HaProxy.....	93
Illustration 33: Principes du recueil de bonnes pratiques ITIL v3.....	105

# INDEX DES TABLEAUX

Tableau 1: Comparatif par critères de choix des types d'enseignement numérique.....	17
Tableau 2: Avantages et inconvénients de deux réseaux d'enseignement isolés.....	34
Tableau 3: Le portefeuille de services du projet CAN/ENT.....	40
Tableau 4: Tableau de répartition des tailles de fichier vidéo du service de cours en ligne.....	45
Tableau 5: Synthèse de l'expression du besoin.....	49
Tableau 6: Les services à prendre en compte lors de la conception.....	52
Tableau 7: État de l'art des solutions de streaming audio et vidéo.....	74
Tableau 8: Synthèse des solutions à réaliser.....	79
Tableau 9: Dépendances entre couches de la plate-forme de diffusion en streaming.....	88
Tableau 10: Synthèse des tests de la plate-forme de diffusion en streaming.....	97
Tableau 11: Synthèse des solutions réalisées.....	100
Tableau 12: Portefeuille des services de l'espace numérique de travail.....	104

# BIBLIOGRAPHIE, WEBOGRAPHIE

- Aspects législatifs de l'obligation de traçabilité

<https://www.odebi.org/lct/Leslogspourlesnuls.html>

- Wikipédia, l'encyclopédie libre

<http://fr.wikipedia.org>

- Consortium ESUP-PORTAIL

<http://www.esup-portail.org>

- Répartiteur de charge HaProxy

<http://haproxy.1wt.eu>

**Fondation Mozilla**

<http://www.mozilla-europe.org/fr>

**Testeur d'application web Selenium**

<http://seleniumhq.org>

**Solution de streaming Wowza Server**

<http://www.wowzamedia.com>

**Librairie de manipulation audio et vidéo ffmpeg**

<http://www.ffmpeg.org>

**Lecteur de fichier Flash en streaming FLV Player**

<http://flv-player.net>

**Serveur de streaming RED5**

<http://code.google.com/p/red5>

**Solution de stockage OpenFiler**

<http://www.openfiler.com>

**Solution de virtualisation VMWare**

<http://www.vmware.com/fr>

**Autorité de certification SSL**

<http://www.thawte.fr>

**Distribution Linux Mandriva**

<http://www.mandriva.com/fr>

**Solution de virtualisation VirtualBox**

<http://www.virtualbox.org>

**Distribution Linux Ubuntu**

<http://ubuntu-fr.org>

**Qualité de service réseau sous Windows**

<http://www.netlimiter.com>

**Scanner de réseau NMAP**

<http://nmap.org>

**Gestionnaire centralisé de configurations Puppet**

<http://www.puppetlabs.com>