Plan de continuité d'activité réseau et protocoles de redondance

Sébastien Lefebvre

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

CENTRE REGIONAL DE TOULOUSE

MÉMOIRE

présenté en vue d'obtenir

le DIPLÔME D'INGÉNIEUR CNAM

SPÉCIALITÉ : Informatique

OPTION : Systèmes, Réseaux et Multimédia

par

Sébastien LEFEBVRE

Plan de continuité d'activité réseau et protocoles de redondance

Soutenu le 5 Février 2013

JURY

PRÉSIDENT :	**Monsieur Pollet, Professeur des universités (CNAM Paris)**
MEMBRES :	**Monsieur Batatia, Maître de conférence (CNAM Toulouse)** **Monsieur Raïf, Maître de conférence (CNAM Toulouse)** **Madame Lecomte, Business Manager (ALTRAN)** **Monsieur Haddad, Business Line Director (ALTRAN)**

REMERCIEMENTS

Je souhaite tout d'abord remercier mes responsables Altran, Madame Fanny Lecomte et Monsieur Nicolas Haddad, qui ont su voir en moi le potentiel nécessaire pour être positionné sur cette mission, en particulier chez ce client.

Je remercie également l'ensemble du service réseau d'Astrium pour son accueil chaleureux et sa disponibilité dans la participation à ce projet d'entreprise.

En particulier, je souhaite adresser mes remerciements à Messieurs Zago et Greiner de m'avoir choisi pour mener à bien ce projet. Ils m'ont fait confiance et laissé autonome tant dans mes choix techniques dans leurs mises en œuvre.

Merci à l'équipe (SPIE) qui opère et gère le réseau au quotidien de m'avoir accordé une place parmi eux, le temps d'un projet. Dans un contexte pas forcément évident, leur expertise et leur maitrise de l'environnement technique m'ont été d'une aide précieuse.

Je remercie l'ensemble des enseignants et l'équipe pédagogique du CNAM de Toulouse pour leur enseignement qui m'a apporté le bagage théorique qui manquait à mon expérience technique. Sans ces connaissances, je n'aurais pu mener à bien ce projet.

Enfin, je souhaite remercier tout particulièrement ma compagne et mes amis qui, par leur patience et leurs encouragements, m'ont permis d'aller au bout de ce projet.

LISTE DES ABREVIATIONS

ADSL: ligne d'abonné numérique à débit asymétrique (asynchronous digital subscriber line)

AFNIC: association française pour le nommage Internet en coopération

ASA: Adaptive Security Appliance, Cisco Cisco PIX

BCI: Business Continuity Instituts

CNAM : Conservatoire National des Arts et Métiers

DNS: Domain Name Server/System

FAI: fournisseur d'accès à Internet

FIFO: First In First Out (premier arrivé, premier servi)

Gbit/s: gigabit par seconde

GUI: graphical user interface

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

ICMP: Internet Control Message Protocol

IGMP: Interior Gateway Routing Protocol

IOS: Internetwork Operating System

IP: Internet Protocol

IPsec: Internet Protocol Security

IT: Information Technology, Informatique

itSMF : it Service Management Forum

ITIL: Information Technology Infrastructure Library

LAN: réseau local (Local Area Network)

MAC: Medium access control

Mbit/s: mégabit par seconde

NTP: Network Time Protocol

OS: Operating System

OSI: Open System Interconnection

PCA : Plan de continuité d'activité

PoP : Point of Presence

PRA : Plan Reprise Activité (ITIL), c'est l'équivalent de la partie informatique d'un PCA (Plan de continuité d'activité)

RAID: Redundant Array of Inexpensive Disks

RFC: Request for comment, appellation des standards IETF de l'Internet, normes rédigées ouvertement

SNMP: Simple Network Management Protocol

SPOF: Single Point Of Failure

SSH: Secure Shell

STP: Spanning-tree Protocol

SYNC: Synchronization

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

VPN: Virtal Pivate Network

WAN: Wide area network

GLOSSAIRE

Adresse MAC : Adresse physique d'une interface réseau fixée par le constructeur qui permet d'identifier de façon unique une machine sur un réseau local.

Appliance : Un appliance est un anglicisme pour évoquer la partie physique (hardware) d'un équipement physique. On parle aussi de boitier.

Backbone : De l'anglais, signifie épine dorsale. Dans les es réseaux de télécommunications, il désigne un réseau fédérateur central sur lequel viennent e rattacher les plus petites entités. Il est par conséquent dimensionné en conséquence avec une large bande passante permettant de gros débits.

Backup : traduction littérale de sauvegarde (sous-entendu : de données), il sert également à désigner un système de redondance pour une application ou un réseau informatique

Datagramme : Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).

DCI: Le Business Continuity Instituts (BCI) a été créé en 1994 et compte aujourd'hui plus de 1750 membres professionnels du management de la continuité d'activité (MCA), originaires de 45 pays. Ils sont notamment à l'origine du livre Management de la continuité d'activité (édité par l'AFNOR en 2007).

Failover (en français, bascule) : mécanisme permettant à 2 équipements primaire/secondaire de fonctionner sur un mode actif/passif. Principe selon lequel la continuité de service est assurée par l'élément secondaire en cas de défaillance du système primaire.

Guest access : ensemble des mécanismes permettant à un utilisateur n'appartenant pas à la société d'obtenir des droits d'accès restreint, comme par exemple la possibilité d'accéder à internet. Cela peut prendre la forme de la mise à disposition d'un compte particuliersur un réseau ou VLANdédié.

Heartbeat (En français battements de cœur) : Messages que s'envoient 2 équipements (dans ce document il s'agira de firewall ASA) afin de signaler régulièrement leur état de santé. Ces informations sont envoyées au travers de messages ICMP ou d'un protocole propriétaire.

HSRP : Hot Standby Router Protocol (HSRP est décrit dans la RFC 2281) est un protocole propriétaire de Cisco disponible sur les équipements de niveau 3 permettant d'assurer une continuité de service en garantissant la disponibilité de la passerelle par défaut dans un sous-réseau même en cas de défaillance du routeur.

IETF : L'Internet Engineering Task Force, est un groupe de travail informel, ouvert à toute personne souhaitant participer activement à la mise au point de standards Internet. L'IETF élabore la plupart des nouveaux standards d'Internet.

itSMF : it Service Management Forum, est une association à but non lucratif, loi française 1901. Ses membres inclus des sociétés utilisatrices de Services Informatique, privées ou publiques et autres SSII, éditeurs de logiciels, etc. Il y a plus de 3000 sociétés dans le monde, membre de l'itSMF. Elle joue un rôle important dans l'élaboration et la promotion des meilleures pratiques de la Gestion de Services Informatiques en France et en particulier ITIL.

LAN : Local Area Network, en français réseau local, ce terme désigne un réseau informatique d'échelle géographique restreinte. Dans le document présent, il s'agit du réseau informatique d'Astrium.

Modèle OSI : Open Systems Interconnection, (« Interconnexion de systèmes ouverts ») est un modèle de communications entre éléments réseaux proposé par l'ISO (International Organization for Standardization). Il découpe en 7 couches les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Open source : Logiciel distribué avec l'intégralité de ses programmes sources, afin que l'ensemble des utilisateurs qui l'emploie (souvent appelé « communauté » de par la mise en commun des connaissances) puisse l'enrichir et le redistribuer à leur tour.

Paquet : Voir Datagramme.

Ping : Ping est un utilitaire d'administration de réseau informatique utilisé pour tester l'accessibilité d'un hôte sur un protocole Internet (IP) et de mesurer le temps d'aller-retour pour les messages envoyés à partir de l'hôte d'origine vers un hôte de destination.

PoP : Point of Presence. Ce sont des points de collecte régionaux au niveau d'un réseau opérateur. Ils centralisent les connexions provenant des DSLAM régionaux, eux-mêmes reliés au backbone opérateur.

Port : Dans une architecture client-serveur, connexion virtuelle permettant d'acheminer les informations directement dans le logiciel d'application approprié de l'ordinateur distant.

Protocole : Ensemble des spécifications décrivant les conventions et les règles à suivre dans un échange de données.

Requête : Ensemble de commandes dont l'exécution permet d'obtenir un résultat.

RFC : Publication de références portant sur le réseau Internet et rédigée par les experts informatiques.

Secure Shell (**SSH**) : est un protocole de communication sécurisé conçu avec l'objectif de remplacer les programmes moins ou non sécurisés comme rlogin, telnet et rsh. Ce protocole impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames échangées sont chiffrées ce rend le contenu inexploitable.

Spanning-Tree : Protocole de niveau 2 défini dans la norme IEEE 802.1D qui s'appuie sur la connaissance de la topologie du réseau et permettant d'éviter les boucles logiques sur un réseau local grâce à différents algorithmes de calcul.

Supervision : Surveillance de l'état d'un réseau et de ses composants. Elle s'appuie principalement sur les protocoles ICMP et SNMP.

Trunk : Appellation Cisco pour une agrégation de lien 802.1q

VPN : Virtual Private Network correspond en fait à une interconnexion de réseaux locaux via une encapsulation des données dans un « tunnel ». Ces données peuvent être chiffrées et ainsi offrir une connexion sécurisée de bout en bout.

VRRP : Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel) est un protocole non propriétaire redondant décrit dans la RFC 5798 dont le but est d'augmenter la disponibilité de la passerelle par défaut pour les hôtes d'un même sous-réseau.

VTP : VLAN Trunking Protocol est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco.

WAN : Un réseau étendu, souvent désigné par l'anglais *Wide Area Network*, est un réseau informatique couvrant une grande zone géographique. Il désigne souvent l'accès à un site distant au travers d'une liaison opérateur. Dans le cas présent, nous étudierons les liaisons inter-sites d'Astrium.

TABLE DES MATIERES

Introduction

«Dans l'ère d'Internet, la fiabilité devient quelque chose que vous devez construire, pas quelque chose que vous achetez. C'est un travail difficile, et cela nécessite de l'intelligence, des compétences et un budget. La fiabilité ne fait pas partie du package de base »[1].

L'informatique a pris, depuis quelques années déjà, une place stratégique au sein des entreprises. Alors qu'il n'était utilisé principalement que pour des applications de messagerie et de la navigation internet, le réseau informatique d'aujourd'hui voit transiter des flux servant aussi bien à la messagerie et le surf internet, qu'au partage de fichiers, aux applications d'entreprise (liées à leur cœur de métier), à la voix ou à la vidéo. À ceux-là viennent s'ajouter les flux de contrôle ou de gestion du réseau qui, même s'ils ne contiennent pas d'information dîtes « métiers », sont nécessaires pour administrer le système d'information, en assurer la maintenance, la supervision ou la sauvegarde.

Autant de données, qui nécessitent un traitement particulier, ont rendu le réseau informatique particulièrement sensible, à tel point que les entreprises (surtout les grandes) consacrent une partie de leur budget de plus en plus conséquente à la maintenance et à l'évolution de leur réseau. La mise en place d'infrastructures robustes permettant de répondre à des critères de performance, tel que les disponibilités du réseau ou le temps de rétablissement du service en cas de coupure, s'inscrivent directement dans le plan de continuité d'activité (équivalent du chapitre informatique du plan de reprise d'activité) de l'entreprise.

L'objet de ce mémoire sera de présenter les outils et protocoles qui permettent d'assurer les mécanismes de redondances et ainsi une continuité de service en cas de panne (voire de double panne) appliquée au réseau d'Astrium. Dans un premier temps, nous aborderons le contexte général dans lequel vient s'inscrire ce projet. Puis, seront présentés les principes généraux qui régissent un plan de continuité d'activité. Dans une troisième partie, nous verrons les différents protocoles choisis pour répondre à notre problématique, en fonction du type d'architecture souhaitée, et comment les intégrer dans la configuration existante. Puis nous conclurons en dressant le bilan du travail effectué d'un point de vue professionnel et personnel.

---

[1] Joel Snyder – Network World Test Alliance -"Reliability: Something you build, not buy"

I CONTEXTE

I.1 ALTRAN

I.1.1 ALTRAN TECHNOLOGIES

Fondé en 1982, Altran est un groupe international de conseil en innovation et ingénierie avancée, leader européen dans son domaine. Sa mission est d'accompagner les entreprises dans leurs projets les plus complexes et leurs démarches de création et de développement de nouveaux produits et services. En 2011, Altran emploie plus de 17000 personnes dans près de 20 pays, dont 9000 en France, son chiffre d'affaires s'élève à 1,4 milliards d'euros.

I.1.2 ALTRAN CIS: CONSULTING IN INFORMATION SYSTEM

La société Altran est organisée autour de quelque 200 filiales autonomes dans leur gestion opérationnelle et leur stratégie commerciale. Le groupe Altran compte aujourd'hui environ 80 filiales opérationnelles. Créée en 2006, Altran CIS (Consulting and Information Services) est une entité transverse qui regroupe l'ensemble des activités de conseil systèmes d'information du groupe Altran.

C'est dans ce contexte qu'Altran m'a positionné sur une mission chez EADS Astrium et m'a permis entre autres de mettre en œuvre ce projet.

I.2 EADS ASTRIUM

I.2.1 EADS

EADS, European Aeronautic Defence and Space company, est la seconde entreprise aéronautique mondiale. Ses domaines de compétence touchent aussi bien le domaine civil que militaire, mais aussi l'espace (avec la filiale Astrium), et les systèmes de défense. EADS est aujourd'hui le leader européen du secteur.

Au total la compagnie emploie plus de 133000 personnes au travers de ces 170 sites de production et bureaux d'étude. Le groupe a dégagé en 2011 un chiffre d'affaires de 5 milliards d'euros.

(6 FRPSUHQG TXDWUH GLYLVLRQV D\DQW FKDFXQH VRQ SURSUH GRPDLQH G¶DFWLYLWp :

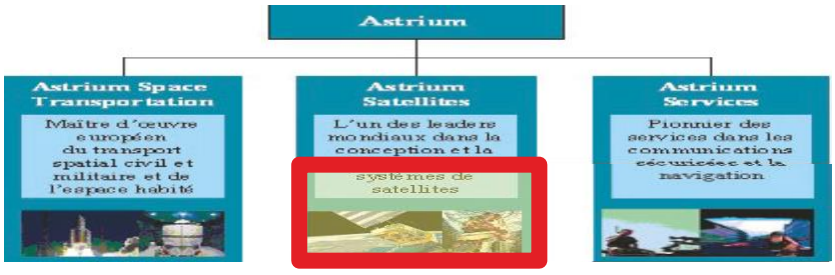
- $LUEXV : FRQVWUXFWLRQ G'DYLRQV, LQFOXDQW OD FRQVWUXFWLRQ G'DYLRQV PLOLWDLUHV GH WUDQVSRUW DX VHLQ G¶$LUEXV 0LOLWDU\.
- **$VWULXP** : FRQVWUXFWLRQ GH ODQFHXUV VSDWLDX[DLQVL TXH GH VDWHOOLWHV GH WpOpFRPPXQLFDWLRQ HW G'REVHUYDWLRQ GH OD WHUUH.
- &DVVLGLDQ : FRQVWUXFWLRQ G'DUPHPHQWV HW G'pTXLSHPHQWV pOHFWURQLTXHV (SUpFpGHPPHQW (6 'HIHQFH & 6HFXULW\).
- (XURFRSWHU : /D FRQVWUXFWLRQ G'KpOLFRSWqUHV FLYLOV HW PLOLWDLUHV.

,.2.2 $675,80

&¶HVW HQ 2003, ORUVTXH %$(6\VWHPV D YHQGX VHV SDUWV j (6, TX¶$VWULXP HVW GHYHQX XQH ILOLDOH j 100% G¶(6. $VWULXP D UpDOLVp XQ FKLIIUH G¶DIIDLUHV HQ 2011 GH 5 PLOOLDUGV G¶HXURV HW XQ FKLIIUH GH SULVH GH FRPPDQGH GH 14,7 PLOOLDUGV G¶HXURV, PDOJUp XQ HQYLURQQHPHQW pFRQRPLTXH GH SOXV HQ SOXV FRPSpWLWLI.

,.2.1 /(6 ',9,6,216[2]

/¶HQVHPEOH GHV DFWLYLWpV VSDWLDOHV G¶(6 RQW pWp UHJURXSpHV VRXV XQH PrPH GLYLVLRQ : (6 $VWULXP, TXL FRPSUHQG PDLQWHQDQW WURLV XQLWpV SUpVHQWHV HQ)UDQFH, PDLV DXVVL HQ $OOHPDJQH HW HQ *UDQGH-%UHWDJQH:



)LJXUH 1 : /HV GLYLVLRQV G¶$VWULXP.

- (6 $VWULXP 6SDFH 7UDQVSRUWDWLRQ (O'H[-(6 6SDFH 7UDQVSRUWDWLRQ) : © F¶HVW OH PDvWUH G¶°XYUH HXURSpHQ GX WUDQVSRUW VSDWLDO FLYLO HW PLOLWDLUH HW GHV YROV KDELWpV. &HWWH XQLWp FRQoRLW, GpYHORSSH HW SURGXLW OHV ODQFHXUV GH OD IDPLOOH $ULDQH, OH

[2] $VWULXP ± /HV DFWLYLWpV - >HQ OLJQH@. 'LVSRQLEOH VXU : KWWS://ZZZ.DVWULXP.HDGV.QHW/IU/RXU-H[SHUWLVHV (FRQVXOWp OH 03/08/2012)

- laboratoire Colombus et le cargo spatial ATV pour la Station Spatiale Internationale, des véhicules de rentrée atmosphérique, les missiles de la Force de dissuasion française, des systèmes propulsifs et des équipements spatiaux. »
- EADS Astrium Services : « c'est le guichet unique sur le marché mondial des services satellitaires, fournisseur de solutions innovantes et sur-mesure dans le domaine des communications sécurisées, des services d'observation de la Terre et de la navigation. »
- EADS Astrium Satellites (l'ex-EADS Astrium d'avant 2006) : « c'est le leader mondial de la conception et de la fabrication de systèmes de satellites. Son activité couvre les systèmes de télécommunications et d'observation de la Terre civils et militaires, les programmes scientifiques et navigations, les moyens sols associés et les équipements spatiaux. »

I.2.2.2 LES SITES

Figure 2: Les sites Astrium à travers le monde.

18 000 personnes sont aujourd'hui employées par Astrium au travers de ses sites en France, en Allemagne, en Grande Bretagne, en Espagne, aux Etats-Unis, en Guyane Française, aux Pays-Bas, en Pologne, en République Tchèque…

Le tableau ci-dessous présente les principaux centres et les activités réalisées par chacun.

Tableau I : Les activités d'Astrium par site.

Pays	Villes	Activités
Allemagne	Brême	Infrastructure spatiale, développe et fabrique l'étage supérieur du lanceur Ariane 5, centre de recherche.
Allemagne	Friedrichshafen	Satellite d'observation de la Terre, électronique, développe et fabrique des installations expérimentales pour la recherche en condition de microgravité.
Allemagne	Lampoldshausen	Fabricant de micro-propulseurs et de systèmes de propulsion.
Allemagne	Ottobrunn	Système de propulsion spatiale, sous-systèmes satellitaires dédiés aux télécommunications, à la navigation et l'observation de la terre.
UK	Stevenage	Satellites de communication civils et militaires, antennes, satellites d'observation de la Terre.
UK	Portsmouth	Instruments radars embarqués, logiciels embarqués, charges utiles de communication.
France	Elancourt	Conception, développement et production d'équipements électroniques, ingénierie d'essai, fabrication de circuits hybrides et multi-puces.
France	Les Mureaux	Maîtrise d'œuvre de grands programmes spatiaux.
France	Toulouse	Conception, assemblage et vérification d'instruments optiques destinés à être embarqués sur les satellites d'observation
Espagne	Barajas	Fabrication de satellite, charges utiles et instruments de bord.
Espagne	Tres Cantos	Conception et fabrication d'équipements électroniques et logiciels pour des applications spatiales.

Ainsi les effectifs sont répartis de la façon suivante :

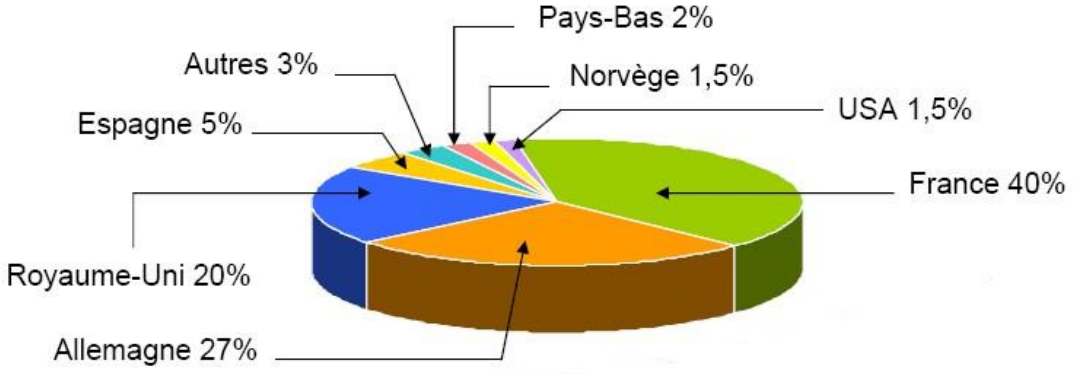
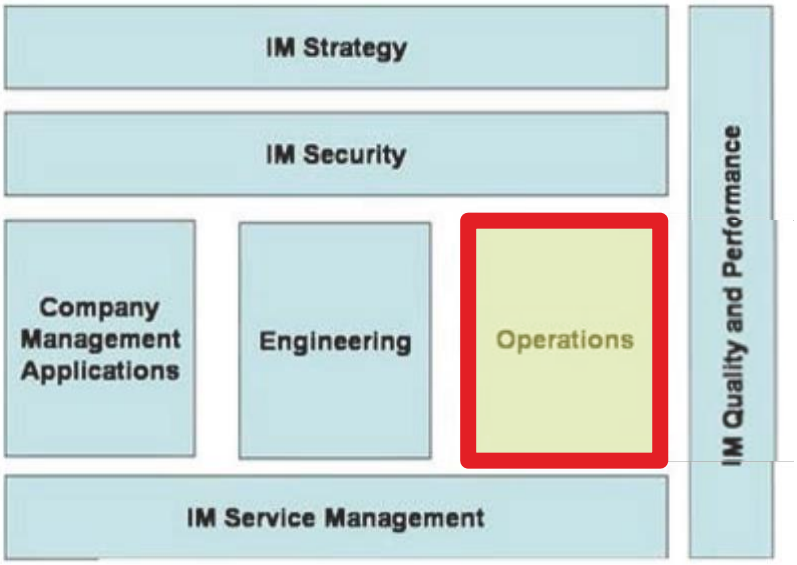


Figure 3 : Répartition des effectifs d'Astrium par pays.

,.2.2.3 ,1)250$7,21 0$1$*(0(17

/H VHUYLFH ,0, FRPSRVp G¶,6 (,QIRUPDWLRQ 6\VWHPV) HW G¶,&7 (,QIRUPDWLRQ &RPPXQLFDWLRQ 7HFKQRORJ\) UpJLW WRXW OH V\VWqPH G¶LQIRUPDWLRQ G¶$VWULXP. /D EUDQFKH RSpUDWLRQ (GH ODTXHOOH MH GpSHQGV) HVW FRQVWLWXpH GH WURLV HQWLWpV:



)LJXUH 4 : 'HVFULSWLRQ GH OD GLYLVLRQ ,QIRUPDWLRQ 0DQDJHPHQW.

- (QG 8VHU 6HUYLFHV: &HWWH pTXLSH V¶RFFXSH GH WRXW FH TXL D DWWUDLW DX 3& HW VHV pTXLSHPHQWV.
- 'DWD &HQWHU 6HUYLFHV: '&6 RSqUH HW HQWUHWLHQW OHV SDUFV GH VHUYHXUV HW EDLHV GH VWRFNDJH VXU GLVTXH TXL KpEHUJHQW WRXWHV OHV DSSOLFDWLRQV ORJLFLHOOHV VWDQGDUG HW GRQQpHV GH O'HQWUHSULVH.
- &RPPXQLFDWLRQ 6HUYLFHV: &H VHUYLFH D SRXU U{OH O'H[SORLWDWLRQ GH WRXWHV OHV LQVWDOODWLRQV GX UpVHDX HW OD SOXSDUW GHV VHUYLFHV YLGpR HW GH OD WpOpSKRQLH. &¶HVW DX VHLQ GH FHWWH pTXLSH TXH YD QDvWUH PRQ SURMHW.

I.3 LE PROJET

I.3.1 DEFINITION DU PROJET

Le cœur du métier d'Astrium implique un niveau élevé de confidentialité des données qui peuvent circuler sur son système d'information. Ce degré de classification fait peser de lourdes contraintes de sécurité sur l'ensemble du réseau. Afin de permettre de s'affranchir des contraintes de sécurité pesant sur la bureautique, un réseau a été construit en parallèle de celui existant.

Cette nouvelle architecture était censée permettre aux personnes, n'ayant pas besoin d'accéder aux moyens informatiques mis à leur disposition, de pouvoir accéder « librement » à internet. Initialement prévu pour fournir des accès internet à quelques projets au travers de quelques dizaines de « box ADSL », le réseau « Internet Projet » n'a cessé de croitre pour héberger une trentaine de projets aujourd'hui. La mise en place d'un accès Internet à 40Mbs a permis de mutualiser ces nombreux points d'accès et donc de supprimer tous les abonnements individuels. Par la suite, de nouveaux services ont fait leur apparition tels que la fourniture d'accès VPN à des partenaires industriels, ou encore la création de comptes temporaires permettant à des invités de se connecter à internet.

Construit progressivement pour répondre à des besoins ponctuels à partir de queues de budget, ce réseau « à plat » n'a jamais été constitué que de quelques dizaines de switches cascadés les uns derrières les autres. Dans la mesure où le service était correctement rendu pour l'ensemble de ses utilisateurs, personne n'avait jamais pris le temps d'étudier de plus près la question du dimensionnement, de l'évolutivité ou de la robustesse de ce réseau. Le faible budget alloué à ce réseau était à l'image de l'importance qu'il avait aux yeux des personnes qui en avait la responsabilité, et proportionnelle à l'implication que pouvaient avoir les équipes opérationnelles quant à sa maintenance.

À force d'évolutions, ce réseau a pris de plus en plus d'importance tant par son nombre de clients que par la criticité des applications qu'il hébergeait. L'année passée, une coupure imprévue sur cet accès internet a permis de se rendre compte de l'impact que pouvait avoir une telle panne sur le business et l'image de l'entreprise auprès de ses clients. Cette année, d'autres évènements d'importances que nous ne pouvons citer ici, ont permis de débloquer un budget conséquent dédié au réseau « « Internet Projet".

Ce projet s'inscrit dans le Plan de Continuité d'Activité de l'entreprise. Il a pour objectif de sécuriser l'architecture actuelle. Autrement dit, de mettre en œuvre une infrastructure réseau permettant d'éviter au maximum les points de panne unique (SPOF).

L'idée est de considérer que l'on devrait disposer des moyens techniques et organisationnels pour pouvoir continuer de rendre le service aux utilisateurs, même dans le cas où le bâtiment, qui héberge tous les services réseau, disparaitrait (incendie, coupure électrique, etc..).

I.3.2 PLANNING DU PROJET

L'étude du projet a démarré au mois de mai de l'année dernière. Une longue période d'étude et de recherche a été nécessaire avant le démarrage de la première phase de mise en œuvre a débuté au mois de Juillet et s'est terminée au mois de Décembre 2012. Aujourd'hui, le projet est toujours en cours de déploiement. Le détail du diagramme de Gantt complet est disponible en Annexe 1.

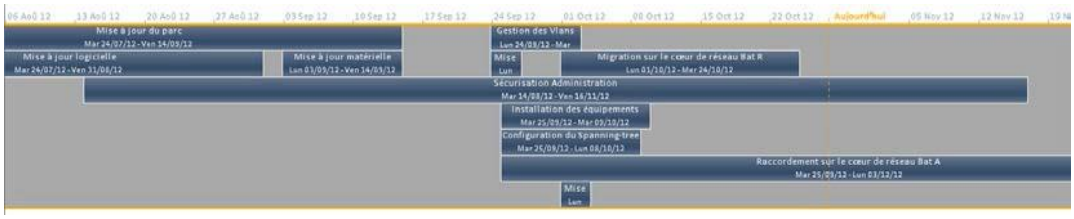


Figure 5 : Chronologie du projet.

II PLAN DE CONTINUITE D'ACTIVITE

II.1 PRINCIPE GENERAL

Selon une étude EMC[3] menée en 2011, au cours de l'année écoulée, 54% des entreprises interrogées ont perdu des données ou subi une interruption de fonctionnement.

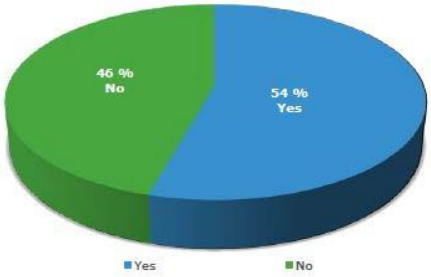


Figure 6 : Pourcentage d'entreprises ayant subi une perte de données ou une interruption de fonctionnement au cours des 12 derniers mois.

Dans 61% des cas, cette interruption a été causée par une panne matérielle. Les catastrophes naturelles et le sabotage sont aussi cités parmi les autres causes d'interruption de fonctionnement ».

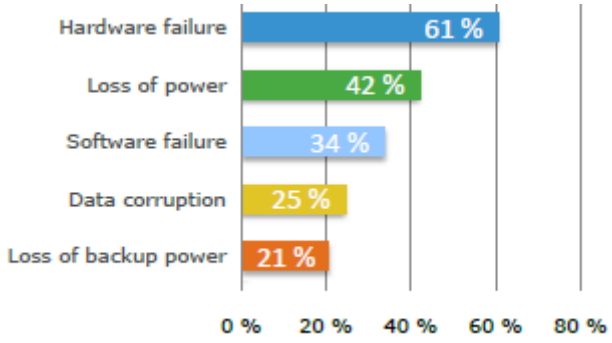


Figure 7 : Causes de la perte de données ou de l'interruption de fonctionnement.[4]

Un PCA (Plan de Continuité d'Activité) est un dispositif organisationnel et technique qui vise à limiter l'impact potentiel d'un sinistre. Le PCA d'une entreprise n'a pas pour objectif de répondre à des incidents ponctuels d'exploitation ou de fonctionnement, il s'agit plutôt de « la solution de la dernière chance » pour faire face à un évènement d'une rare ampleur telle qu'une catastrophe naturelle ou encore un incendie (destruction d'un bâtiment par exemple). Prévoir l'imprévisible et pouvoir y apporter une solution efficace lorsqu'un sinistre a touché le cœur de l'entreprise. En fonction de sa taille, une entreprise

[3] The Disaster Recovery Survey 2011: Europe-commissioned by EMC
[4] Question posée aux 54% des entreprises concernées.

peut avoir à mettre en œuvre différents plan de continuité d'activité concernant par exemple, différents départements ou services de celle-ci. Le PCA a pour mission de garantir la sécurité et la continuité des opérations métiers et doit couvrir toutes les fonctions vitales d'une l'entreprise.

Ce plan doit permettre de réduire, voire maitriser l'impact d'un sinistre sur l'activité et la productivité de l'entreprise. La figure ci-dessous illustre les principaux[5] impacts constatés, avec en tête de liste la perte de productivité et de revenus.

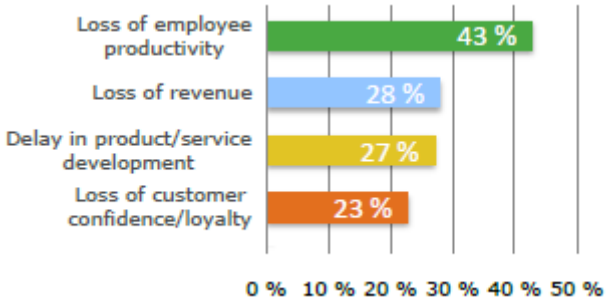


Figure 8 : Conséquences de la perte de données ou de l'interruption de fonctionnement.

De plus, comme le montre le diagramme ci-dessous, ceux-ci, avec 49%, concernent principalement le secteur de l'informatique et des télécommunications.

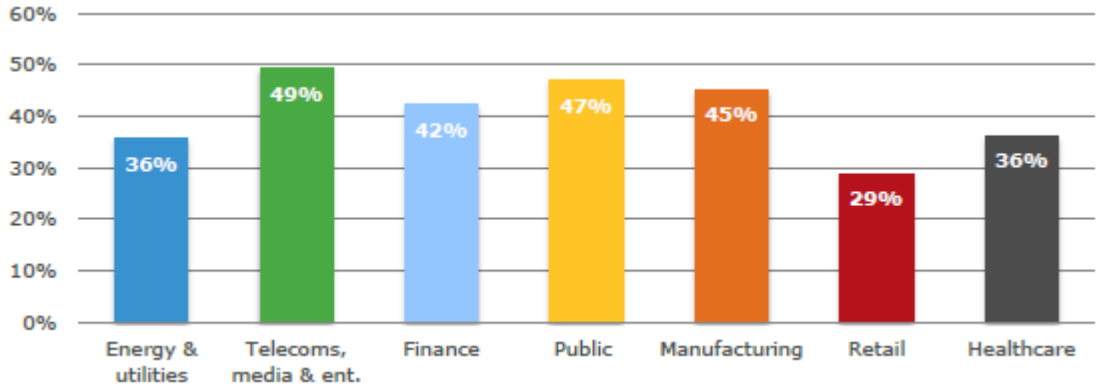


Figure 9 : Secteurs impactés par la perte de productivité

[5] Extrait de The Disaster Recovery Survey 2011: Europe-commissioned by EMC, page 22.

Par ailleurs, afin de situer encore davantage notre projet dans le contexte actuel, le diagramme ci-dessous représente la taille des entreprises les plus impactées. On peut constater que celles de plus de 3000 salariés sont plus particulièrement touchées.

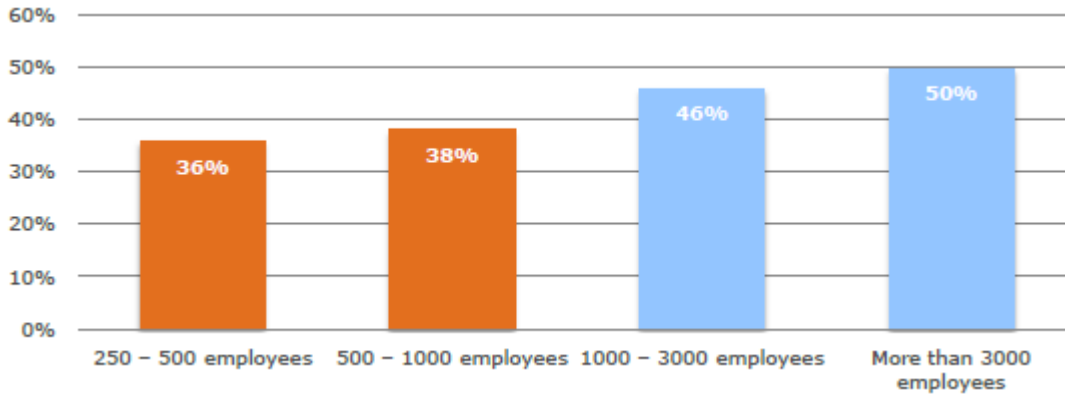


Figure 10 : Impact en fonction de la taille de l'entreprise

Ceci pour illustrer que la société Astrium correspond tout à fait dans la cible décrite dans les quelques graphiques précédents. Ce projet de PCA s'inscrit naturellement dans la continuité des évolutions nécessaires à son système d'information. Dans le cadre de cette étude, le plan de continuité d'activité se limite aux services informatiques et télécoms. Aussi nous détaillerons amplement l'analyse des risques, pour aborder plus rapidement le plan de continuité (plus administratif) en lui-même.

II.2 METHODOLOGIE

La méthodologie choisie pour effectuer notre plan de continuité s'inspire largement des référentiels ITIL[6].

La construction du plan de continuité d'activité s'appuie sur les mêmes étapes que celles d'un projet, à savoir :

- Analyse : Analyse des étapes précédentes
- Conception : Collecte des besoins internes en termes de continuité/disponibilité puis proposition d'une solution.
- Validation : Validation de la solution

[6] L'ensemble des documents utilisés pour rédiger cette partie ont été extrait de la littérature mise à disposition par le groupe de travail itSMF. S'agissant d'une méthodologie, il est donc normal d'y retrouver des similitudes tant sur le fond que sur la forme.

II.2.1 ANALYSE DES RISQUES

La mise en œuvre d'un plan de continuité d'activité implique de suivre une méthodologie avec des étapes « clés » dont l'analyse des risques est la pierre angulaire. En effet, avant de démarrer quoi que ce soit, il est indispensable de mener une étude approfondie.

L'analyse des risques à proprement parlé, a été initiée suite aux évènements rencontrés l'année dernière et cités en introduction. Ce sont donc les deux incidents majeurs qui ont permis de mesurer l'urgence de la situation et ainsi de déclencher l'étude et la mise en place un plan d'action à court et à moyen terme.

II.2.1.1 DEFINITION DU PERIMETRE

La première étape consiste à définir le périmètre sur lequel sera menée l'analyse de risques. Premièrement, un inventaire des « actifs » (matériels, logiciels, équipes de support, données, interfaces, processus) doit être effectué.

Une fois l'environnement opérationnel établi, il reste à identifier les contraintes fonctionnelles (métier), l'utilisation qui en est faite, les politiques qui s'y appliquent, l'architecture du système, la topologie du réseau, le stockage des données, les flux de données, les contrôles techniques opérés, la sécurité physique.

Dans notre cas, la méthode de collecte de ces informations a pris la forme d'interview auprès des différents acteurs de ce réseau et plus particulièrement des équipes s'occupant des opérations et des études. Afin de compléter cette étude, les documentations liées à ce réseau ont été consultées et assimilées (architectures, matrices de flux, schémas réseau, etc…). Même si pour des questions pratiques (de planning notamment) il n'en a pas été fait usage, des questionnaires aurait pu également pu être proposés aux utilisateurs positionnés sur des environnements « projets métiers et opérationnels ».

Dans la littérature fournie par ITIL, ils sont classés[7] sous le processus Component Capacity Management, pour Gestion de la capacité des composants. Les composants sont des éléments d'infrastructure de services IT, comme les disques durs, la bande passante réseau, les transformateurs, postes de travail, les connexions réseau, etc. Un des principaux objectifs du component capacity management est la surveillance des composants pour

[7] ITIL, dans sa version 3, propose de diviser le processus « Capacity Management » en 3 sous-processus (Component, Service et Business)

assurer une capacité suffisante sur place pour exercer les fonctions respectives de manière optimale.

Quant à la gestion des services (Service capacity Management), les services informatiques incluent e-mail, Internet, téléphonie, messagerie, etc… Dans le précédent sous-processus, nous avons examiné les niveaux de capacité des composants individuels - les serveurs, les routeurs, les commutateurs, etc. La gestion de la capacité de service nécessite de faire un parallèle avec cette étape. Ainsi, sur un service de messagerie, l'objectif de gestion des capacités est de s'assurer que le service de courrier électronique est suffisamment dimensionné pour fonctionner correctement. Cela peut se traduire par la mise en commun de serveurs individuels, ou leur séparation, l'installation d'équilibreurs de charge, pour faire en sorte que leurs capacités sont suffisantes pour fournir une qualité de service optimale.

Les accords de niveau de service (SLA) traitent de capacités de service et pas de celle de ses composants. Une fois la capacité de service définie, la capacité des composants doit être alignée pour répondre aux exigences de service.

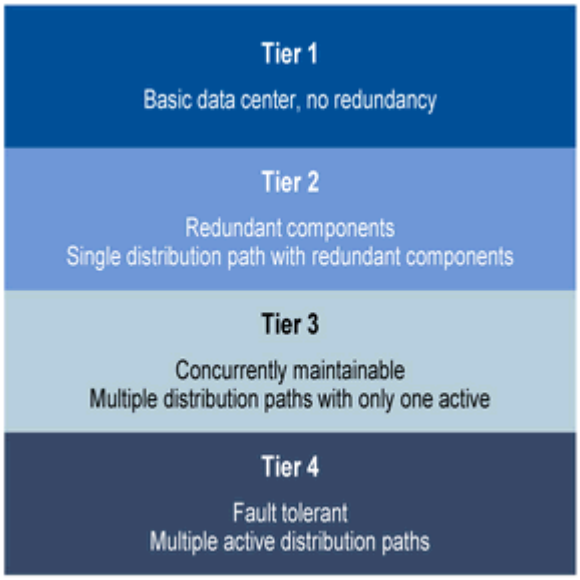


Figure 11 : Périmètre et niveau de redondance attendu

Cette première étape a permis d'affiner le périmètre de notre analyse et le réseau Internet Projet ne fournit pas aujourd'hui de services IP (DNS, DHCP, Proxy,…), ou nécessitant des infrastructures lourdes (serveurs Active Directory, partages de fichiers,…). De fait, il est entièrement sous la responsabilité du service réseau, et seuls les équipements réseau sont susceptibles d'altérer son bon fonctionnement.

II.2.1.2 IDENTIFICATION DES MENACES

Selon ITIL[8], « une menace est la cause potentielle d'une vulnérabilité. Une vulnérabilité est une faiblesse (faille) qui peut être intentionnellement ou non exploitée. Une menace associée à une vulnérabilité potentielle engendre un risque ».

L'identification des menaces consiste à identifier les événements ou circonstances qui pourraient détériorer l'environnement IT.

Cette étape doit autant prendre en compte les menaces environnementales (inondation, feu, explosion) que le facteur humain (piratage informatique, erreurs intentionnelles ou non, etc.).

Dans le cadre de cette étude, nous prenons comme hypothèse de départ la disparition possible du bâtiment où sont installés les moyens réseaux et télécoms. Ce cas permet d'avoir une vision très complète des impacts possibles sur le système d'information.

II.2.1.3 IDENTIFICATION DES VULNERABILITES

Est appelée vulnérabilité[9] « toute faille ou faiblesse dans les procédures de sécurité, dans la conception; la mise en œuvre, ou les contrôles internes d'un système et qui pourraient être exploités et conduire à une brèche de sécurité du système ».

Pour chacune des menaces citées précédemment (une seule dans notre cas), il faut maintenant dresser une liste des vulnérabilités, les analyser afin de déterminer celles qui, si elles étaient exploitées, pourraient impacter de façon plus ou moins importante notre environnement IT.

ITIL nous propose comme méthode d'identification des vulnérabilités, la détermination de leur(s) cause(s) potentielle(s), l'analyse de la performance des processus

[8] Définition extraite de la *Méthodologie d'évaluation des risques (ITIL 2011)*
[9] Définition extraite de la *Méthodologie d'évaluation des risques (ITIL 2011)*

de contrôle de sécurité, et la mise en place d'une liste exhaustive d'exigences sécuritaires à respecter.

En fonction de chaque situation, il est nécessaire d'adapter cette méthodologie en s'appliquant davantage à prendre connaissance de l'environnement dans lequel elle s'applique. Trois typologies distinctes de l'environnement IT sont à prendre en compte :

- Phase de conception
- Phase de déploiement
- Phase opérationnelle

À mesure que l'on avance, l'analyse effectuée doit prendre en considération davantage l'historique et il convient de faire un focus sur les mesures de sécurité intégrées dans les spécifications qui ont permis chaque passage à l'étape supérieure.

Il existe des outils de détection automatique sous formes logicielles (Nessus, Npmap, Nikto, etc…) ou sous forme d'appliance (sondes réseau par exemple), qui aujourd'hui facilite grandement l'identification des vulnérabilités (d'un point de vue technique) et permet un gain de temps non négligeable[10], puisque leur rôle est à la fois de scanner le réseau à intervalles réguliers, mais aussi de capturer et d'analyser l'ensemble des trames circulant sur le système d'information pour en déterminer les failles.

S'agissant de répertorier les vulnérabilités organisationnelles ou humaines, aucun outil n'existe à ce jour (à notre connaissance) pour en permettre l'analyse. Bien qu'ayant été réalisées au court de ce projet, nous n'aborderons pas en détail les rapports d'audits et d'interview dans cette partie.

Pour des raisons de confidentialités, l'analyse des vulnérabilités techniques, notamment en matière de sécurité, ne figure pas ici. En effet, elle fait partie d'un autre projet[11] à part entière, dans lequel l'analyse des vulnérabilités de sécurité y est détaillée. Ainsi, nous nous focaliserons davantage sur les aspects opérationnels décrits ci-après.

II.2.1.3.1 ACCES A INTERNET

[10] Quelques années en arrière, ces analyses se pratiquaient en scannant manuellement le réseau grâce à des outils

[11] Ce projet a permis de mettre en exergue des faiblesses au niveau de la sécurité. Ainsi, un autre projet ayant pour but de sécuriser le réseau Internet Projet a été ouvert. Son degré de confidentialité étant élevé, nous ne l'aborderons pas dans ce document.

La mutualisation des accès internet a été un grand pas vers la fiabilisation du réseau en les réduisant à un seul point d'entrée unique géré par un même opérateur. Cependant, la limite de cette solution est d'accroitre considérablement le nombre d'utilisateurs impactés en cas de coupure de l'accès à Internet. Et l'histoire a montré qu'un seul accès pouvait être une réelle source de problème sur laquelle le client a peu de solutions à apporter.

II.2.1.3.2 POINTS DE PANNE UNIQUE

Lors de cette analyse, il est apparu que ce réseau comportait autant de points de panne unique (en Anglais SPOF = Single Point Of Failure) qu'il y avait d'équipements. En effet, l'architecture a évolué au fil des années avec pour objectif de répondre aux besoins ponctuels, mais néanmoins réguliers de certains projets. Aucune priorité n'étant positionnée sur ce réseau, le budget alloué à son évolution n'a pas permis de repenser son architecture avant ce jour.

II.2.1.3.3 MECANISMES DE REDONDANCE

Il n'existe aujourd'hui aucun mécanisme de redondance à chaud[12] qui soit sous la maitrise d'IM (Information Management). En effet, du fait de la présence de points de panne unique, le besoin n'existait pas jusqu'à ce jour. En cas de défaillance de l'un des équipements, celui-ci est remplacé manuellement par un autre positionné « sur étagère ». Sa configuration est « poussée » manuellement avant sa mise en service.

II.2.1.4 METHODES DE CONTROLES

Une fois les vulnérabilités identifiées, il est nécessaire pour l'entreprise d'analyser les contrôles mis en œuvre ou à mettre en œuvre pour réduire ou éliminer le risque. Cette analyse concerne essentiellement les aspects sécurité. Pour des raisons de confidentialité, nous aborderons dans cette partie uniquement les concepts théoriques, sans les illustrer au travers d'exemples.

[12] On appelle redondance à chaud un mécanisme qui permet, de façon automatique, de continuer de rendre le service en cas de défaillance du système principal.

À ce stade, il est important d'ajuster les méthodes de contrôle en regard du niveau de probabilité de concrétisation du risque, ou de l'intérêt que peut représenter la menace pour le hacker[13]. Il est également possible de valider la nécessité de réduire l'impact d'un risque donné.

II.2.1.4.1 METHODES DE CONTROLE

Selon la méthodologie d'évaluation des risques, proposée par ITIL, « les contrôles de sécurité regroupent les dispositifs techniques et organisationnels. Les contrôles techniques sont ceux qui sont embarqués dans les matériels, logiciels, tels que les mécanismes d'identification, d'authentification, de cryptage, de détection d'intrusion. Les contrôles "non techniques" regroupent les politiques et procédures de sécurité, les contrôles opérationnels, les processus ».

II.2.1.4.2 CATEGORIES DES CONTROLES

Deux catégories se distinguent parmi les différentes méthodes de contrôles, les "proactives" (préventives) et les "réactives".

Dans le premier cas, il s'agit d'anticiper la violation, ou l'exploitation d'une faille du système, ou encore de prévenir des prémices d'un dysfonctionnement susceptibles de représenter une menace. Ces éléments sont, de préférence, mis en place dès la conception du réseau informatique. Dans notre cas il s'agit d'anticiper des cas de pannes uniques en mettant en œuvre des mécanismes de redondance dynamiques.

La conception du réseau en étoile ne nécessitait aucunement la mise en place de mécanismes spécifiques ou de l'utilisation de protocoles particuliers. L'architecture « à plat » constituée d'une succession de switches cascadés est aujourd'hui sujette à de nombreuses boucles réseaux, et autres pannes de plus ou moins grande ampleur et force est de constater qu'au mécanisme de contrôle « pro-actif », n'existe pour l'instant.

Dans le second, la vulnérabilité a déjà été exploitée, et il s'agit maintenant d'en limiter l'impact. Le contrôle peut être réalisé grâce à des outils de supervision ou encore (comme vu précédemment) grâce à des logiciels embarqués ou non, qui vont aller tester régulièrement certains aspects du réseau.

[13] Attaquant

Sur le réseau actuel, la supervision est assurée par un logiciel gratuit effectuant des requêtes ICMP et SNMP. Celui-ci est configuré pour vérifier l'état « réseau » d'un équipement en envoyant des demandes d'écho régulières (PING). Le protocole SNMP ne sert qu'à récupérer des statistiques sur les liens d'interconnexions « inter-switches ». L'interprétation des statistiques est réalisée manuellement de façon ponctuelle, souvent lors de l'apparition d'un incident.

II.2.1.5 DETERMINATION DES PROBABILITES

Comme indiqué dans la partie II.2.1.3 Identifications des vulnérabilités, il est également nécessaire de qualifier la probabilité qu'une vulnérabilité potentielle soit exploitée. Trois niveaux sont définis : élevée, moyenne ou faible.

- **Élevé** : La menace est très importante et facilement exploitable. Les contrôles existants pour prévenir les vulnérabilités sont insuffisants et/ou inefficaces.
- **Moyenne :** La menace est importante et facilement exploitable. Mais les contrôles sont en place pour éliminer l'exploitation de la vulnérabilité.
- **Faible :** La menace est peu importante et les contrôles sont en place pour éliminer l'exploitation de la vulnérabilité.

S'agissant de la capacité à limiter l'impact des points de panne unique, nous nous sommes appuyés sur les évènements récents (un par an durant les deux dernières années), pour en déduire que le niveau de probabilité que cela se reproduise est **élevé**. Par ailleurs, l'existence et la priorité élevée de ce projet justifient également ce choix.

II.2.1.6 ANALYSE D'IMPACT

Cette étape a pour but de cibler les effets indésirables, voire néfastes, résultant de l'exploitation de l'une des vulnérabilités citées précédemment. Avant de démarrer cette analyse, il est nécessaire de se remémorer le périmètre défini plus haut, dans lequel il est question de Service Capacity Management et Component Capacity Management. Il est ici question d'évaluer l'importance des actifs ou leur valeur vénale, la criticité des systèmes et données, etc. L'analyse de ces éléments nous amène à pouvoir évaluer l'impact potentiel sur ces informations en termes d'intégrité, de confidentialité et de disponibilité nous permettra de mesurer le niveau de risque.

Dans le cadre de cette étude, nous nous focaliserons sur la perte de disponibilité. En effet, le fonctionnement et la productivité d'une entreprise peuvent être grandement compromis lorsque les données qu'elle traite sont inaccessibles.

À l'instar des vulnérabilités, le niveau d'impact des risques peut être évalué selon trois niveaux de criticité. À noter qu'il est difficile de mesurer l'impact sur l'image d'une entreprise ou sa notoriété, et que le résultat serait plutôt subjectif.

- **Élevé :** Perte d'actifs très couteux, obstacle important dans la mission de l'organisation, ou altération de la réputation.
- **Moyen :** Perte d'actifs, obstacle important dans la mission de l'organisation, ou altération sa réputation.
- **Faible :** Perte de certains matériels ou actifs et potentielle affectation de la réputation.

En regard du périmètre défini, l'analyse nous permet d'établir un niveau **moyen** d'impact tant sur l'image que sur la productivité.

II.2.1.7 DETERMINATION DU RISQUE

Une fois la probabilité de voir l'évènement se produire évaluée, et l'impact potentiel sur l'environnement IT mesuré, il faut maintenant déterminer le facteur risque.

La méthode consiste à pondérer la menace entre 1 et 5 (du plus faible au plus fort) et à déterminer l'impact entre 1 et 5. Le facteur de ces deux valeurs indique le niveau de risque.

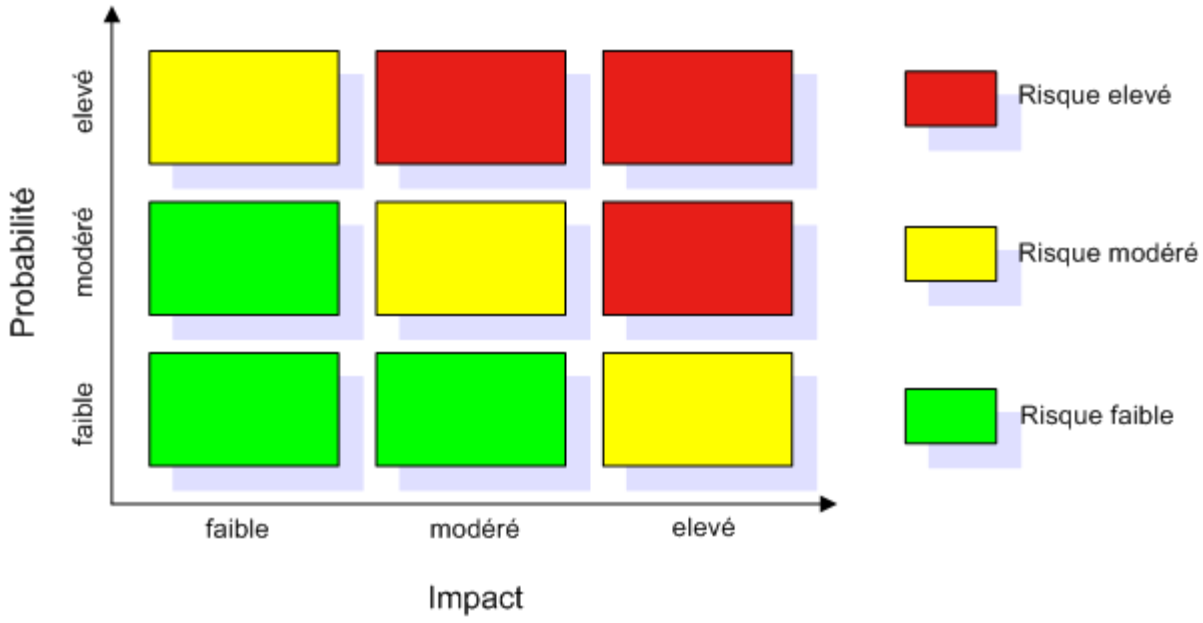


Figure 12 : Exemple de grille de risque

Description des niveaux de risque et actions associées :

- **Élevé :** Mise en œuvre d'une action corrective immédiate.
- **Modéré :** Actions à planifier dans un délai raisonnable.
- **Faible :** soit il peut être accepté, soit faire l'objet d'actions correctives.

Dans notre cas, le risque est **modéré**, un plan d'action à moyen terme a donc été établi, et l'objet de ce mémoire constitue l'une des solutions proposées.

II.2.1.8 SYNTHESE ET PLAN D'ACTION

La principale faiblesse du réseau internet projet réside dans son incapacité à répondre aux cas de pannes uniques. L'analyse de risques a permis de définir le niveau de criticité global du réseau internet projet qui nous impose de rendre le service dans les quatre heures suivant l'interruption. Aussi, il a été convenu de mettre en œuvre un environnement informatique fonctionnant sur un mode actif-passif pour une haute disponibilité maximum. Ainsi les projets sensibles aux interruptions de services, seront assurés de la reprise rapide voire transparente des systèmes requis.

Un nouvel accès internet doit être installé à partir d'un nouveau PoP (point of présence) opérateur, ce qui permettra de s'affranchir également d'une panne opérateur. S'agissant du même opérateur, un contrat de service peut-être mis en place avec le fournisseur d'accès pour définir le temps rétablissement de ses propres équipements. Les méthodes utilisées pour maintenir le service seront détaillées en troisième partie de ce document.

Afin de répondre à la majorité des cas de pannes et assurer une redondance parfaite, cet environnement passif sera localisé dans une salle informatique prévue à cet effet et située dans un autre bâtiment. Une baie technique mise à disposition du projet sera raccordée sur un réseau électrique différent de celui dédié aux moyens actifs. Ainsi, la défaillance du système d'alimentation principal n'altèrera pas les moyens de secours. Par ailleurs, chacun des équipements réseau sera lui-même alimenté par un onduleur. L'autonomie d'une à deux heures permet de répondre également à des pannes électriques de courte durée.

Les éléments actifs seront doublés et installés également dans ces locaux techniques. Doubler le matériel ne suffit pas à supprimer les SPOF sur le réseau. Pour ce faire, il est nécessaire de mettre en place des solutions techniques particulières, en s'appuyant sur l'utilisation de protocoles spécifiques tels que spanning-tree, hsrp ou autre… À noter que l'utilisation de ces protocoles peut impliquer la mise à niveau des systèmes d'exploitation[14] de ces équipements. Les techniques et protocoles utilisés seront décrits plus loin dans ce document.

[14] Le système d'exploitation de l'ensemble du parc est IOS de chez Cisco (anciennement CatOS)

Une fois ces bases établies, d'autres actions seront à prévoir à moyen terme, l'allocation du budget et des ressources n'étant pas suffisante à ce jour pour toutes les réaliser. Des sondes doivent être positionnées afin d'obtenir de informations de métrologie, notamment sur l'utilisation les liens opérateurs. L'outil de supervision est prévu d'être remplacé afin de pouvoir bénéficier des informations contenues dans les trap snmp (pas de trap receiver existant), et de superviser de façon simplifiée l'ensemble des équipements (support du spanning-tree par exemple). À titre informatif, il est également prévu d'installer de nouveau services IP de type DNS, proxy ou DHCP. Enfin le serveur depuis lequel les équipements sont gérés doit également être redondé (une solution virtuelle est déjà à l'étude).

II.2.2 PLAN DE CONTINUITE D'ACTIVITE (DRP/PCA)

Maintenant que le plan d'action est défini, et les échéances positionnées, il reste à rédiger le plan de continuité d'activité. Celui-ci est constitué de 4 phases majeures. Bien qu'elles représentent la finalité de cette analyse de risques, ces phases ne seront décrites que brièvement ci-après. En effet, leur contenu, plutôt administratif, n'est pas directement lié à notre projet d'étude. Aussi, le document complet permettant de mieux comprendre les choix effectués est disponible en Annexe 2.

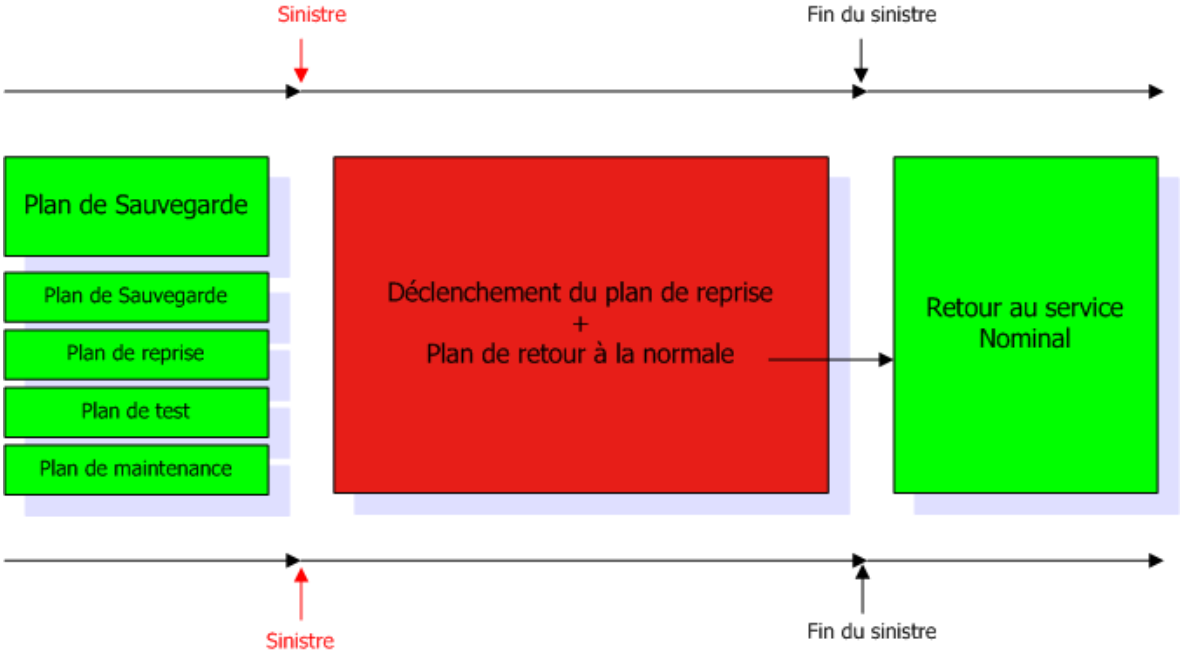


Figure 13 : Phases du plan de continuité d'activité

II.2.2.1 PLAN DE SAUVEGARDE

Le plan de sauvegarde correspond à la phase préparatoire durant laquelle il faut identifier les causes potentielles de sinistres et construire les solutions appropriées pour y répondre de la façon la plus adaptée possible.

Dans notre cas, nous avons pris comme hypothèse de départ le pire des scénarios, à savoir, la destruction complète du bâtiment hébergeant les salles réseau informatique. La réponse choisie est un mode de continuité intégrale avec une coupure de service n'excédant pas quatre heures.

II.2.2.2 PLAN DE SECOURS

L'objectif du plan de secours est de réduire ou limiter l'impact d'un sinistre. L'étape de construction est donc la clé de voute des opérations qui seront réalisées à terme.

Le plan de secours peut être découpé en 3 parties.

II.2.2.2.1 DISPOSITIONS TECHNIQUES ET ARCHITECTURALE

Les dispositions techniques et architecturales couvrent l'ensemble des moyens techniques à mettre à déployer en amont.

Comme il a été défini plus haut, le périmètre de notre PCA couvrira principalement:

- Les salles techniques,
- Les équipements réseau,
- L'accès Internet mis à disposition par IM (Information Management).

II.2.2.2.2 DISPOSITIONS PROCEDURALES

Une fois le dispositif technique établi, la difficulté du projet réside dans la capacité d'organisation de l'entreprise à faire face à une situation complexe, durant laquelle les moyes de communications ou les locaux peuvent être endommagés, voire inaccessibles.

C'est dans ce but qu'il est indispensable de mettre en place en amont toutes les procédures d'intervenions et documentations nécessaires pour faire face à un sinistre lorsqu'il se produit. L'ensemble de ces procédures et processus doit être formalisé, diffusé, compris et maitrisé par l'ensemble des acteurs du plan de continuité d'activité

II.2.2.2.3 DISPOSITIONS ORGANISATIONNELLES

Les dispositions organisationnelles définissent l'organisation à mettre en place pendant la période de crise. Elles sont censées répertorier de manières exhaustives toutes les démarches à suivre, notamment d'un point de vue administratif afin d'être en conformité avec la législation et plus précisément du Code du travail. Elles concernent entre autres :

- ***Habilitation***
- ***Formation***
- ***Cellule de crise***
- ***Contrats de travail***

II.2.2.3 PLAN DE REPRISE

Le plan de reprise est en fait, la mise en pratique des actions définies dans le plan de sauvegarde, en situation réelle, c'est-à-dire lors de l'apparition du sinistre.

II.2.2.4 PLAN DE RETOUR A LA NORMALE

Le plan de retour à la normale inventorie l'ensemble des opérations à réaliser pour revenir à une situation nominale (antérieure au sinistre). Il s'agira de remettre en état de fonctionnement l'ensemble des services, en fonction des critères de disponibilités (SLAs), et en respectant les priorités définies dans le plan de reprise.

II.2.2.5 PLAN DE TESTS

Un plan de continuité d'activité s'appuie sur une « photo » à un instant « T » du système. Aussi, il est indispensable de le faire évoluer à chaque modification effectuée sur le SI (pour la partie nous concernant), mais aussi en regard de la législation qui pourrait avoir changé entre le moment de la création du document et sa mise en œuvre. Si l'on veut pouvoir valider l'ensemble du PCA, il est indispensable de le dérouler lors de cas concrets, et ce, le plus régulièrement possible.

II.2.2.5.1 TEST THEORIQUE

Le test théorique est un test effectué « sur le papier », par conséquent, il ne perturbe pas le fonctionnement du système et ne nécessite pas de prévoir une interruption de service. Il s'agit d'une première étape servant à valider le contenu du plan de reprise. Il est important de dérouler correctement le test afin d'avoir une réelle vision de la bonne chronologie des étapes ou encore de la complétude ou la mise à jour des documents (techniques, procéduraux, ou organisationnels).

II.2.2.5.2 PRE-TESTS ET TESTS PARTIELS

Le test partiel comme son nom l'indique a pour vocation de lancer des tests unitaires très ciblés sur une partie des dispositions de secours. L'idée est de traiter chacune des étapes du plan de reprise, de façon séquentielle afin de limiter l'impact sur le SI, d'en relever les erreurs pour pouvoir mettre à jour les documents.

II.2.2.5.3 TEST COMPLET

Enfin le test complet, quant à lui a pour but de valider le plan de continuité d'activité dans son ensemble. Il doit pouvoir être réalisé dans les conditions réelles d'un sinistre. Seul ce test complet permet d'avoir la garantie de son efficacité.

Considérer comme trop couteuse la simulation d'un sinistre serait commettre l'erreur de beaucoup (trop) d'entreprises qui se retrouve le jour « J » avec un document partiellement faux voire complètement obsolète. La réussite d'un plan de continuité d'activité réside dans son adaptation face aux changements techniques et/ou organisationnels.

II.2.2.6 PLAN DE MAINTENANCE

L'évolution constante de l'environnement technologique, de la législation en vigueur, ou encore son leur organisation propre obligent les entreprises à adapter leur système d'information régulièrement pour proposer de nouveaux services, un niveau de sécurité supérieur, ou simplement se tenir au fait des dernières innovations techniques.

Autant de paramètres qu'il faut prendre en compte et intégrer dans le plan de continuité d'activité. Celui-ci est soumis aux cycles de vie des différents éléments qui le composent. Ainsi, il faudra l'adapter et réitérer les différents plans de tests aussi souvent que nécessaire, le plan de maintenance est là pour en garantir le suivi.

III DE LA THEORIE A LA PRATIQUE

L'analyse de risques étant achevée, le plan d'actions a été défini. À partir de celui-ci, principalement accès sur la redondance et la sécurité[15], nous devons élaborer une stratégie de mise en œuvre. Le choix qui a été fait pour structurer notre démarche est de s'inspirer du modèle hiérarchique proposé par Cisco.

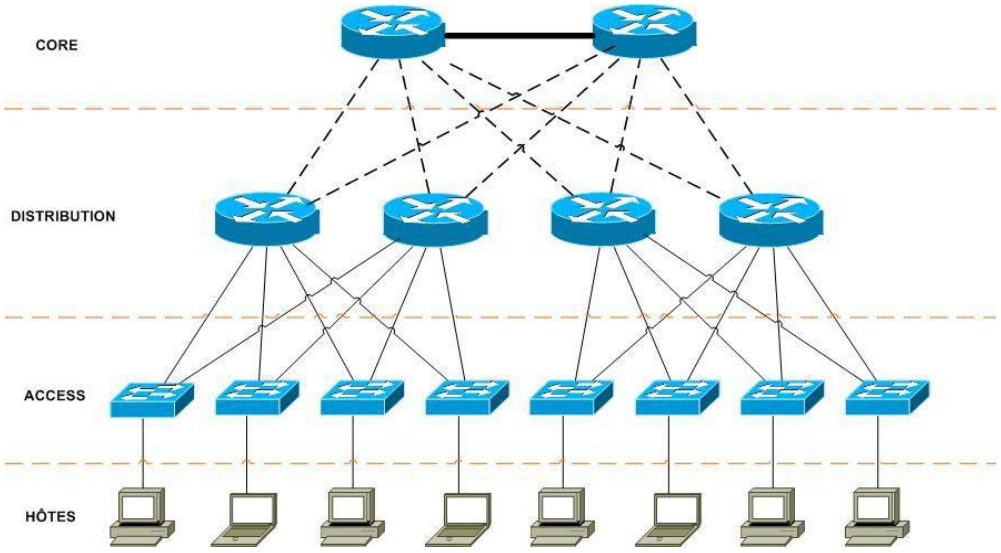


Figure 14 : Modèle hiérarchique en 3 couches, proposé par Cisco

Sa conception va nous permettre de faire une analogie, non pas avec les protocoles utilisés (comme permettrait de le faire le modèle OSI), mais plutôt avec les types d'équipements existants sur le réseau Internet Projet, et le service qu'ils rendent. En d'autres termes, nous allons étudier les mécanismes de redondance qui ont été mis en place au niveau des couches accès, distribution et cœur[16] de réseau. À chacune d'entre elles sont associé un ou plusieurs types d'équipements existants sur le réseau Internet Projet. C'est à partir de ces éléments que certains protocoles plutôt que d'autres ont été choisis pour pouvoir répondre à notre problématique de redondance. L'objet de cette partie est de montrer comment mettre en œuvre une architecture complètement redondée en s'appuyant ces protocoles.

L'approche générale étant posée, nous allons maintenant aborder la construction du projet en commençant par décrire la phase préparatoire (indispensable), avant d'enchainer sur les différentes solutions mises en place sur le réseau Internet Projet.

[15] Des actions sont actuellement en cours pour améliorer la sécurité du réseau Internet Projet. En revanche, pour des raisons de confidentialité, le sujet n'est pas traité dans ce document.
[16] La couche cœur sera souvent appelée core par anglicisme.

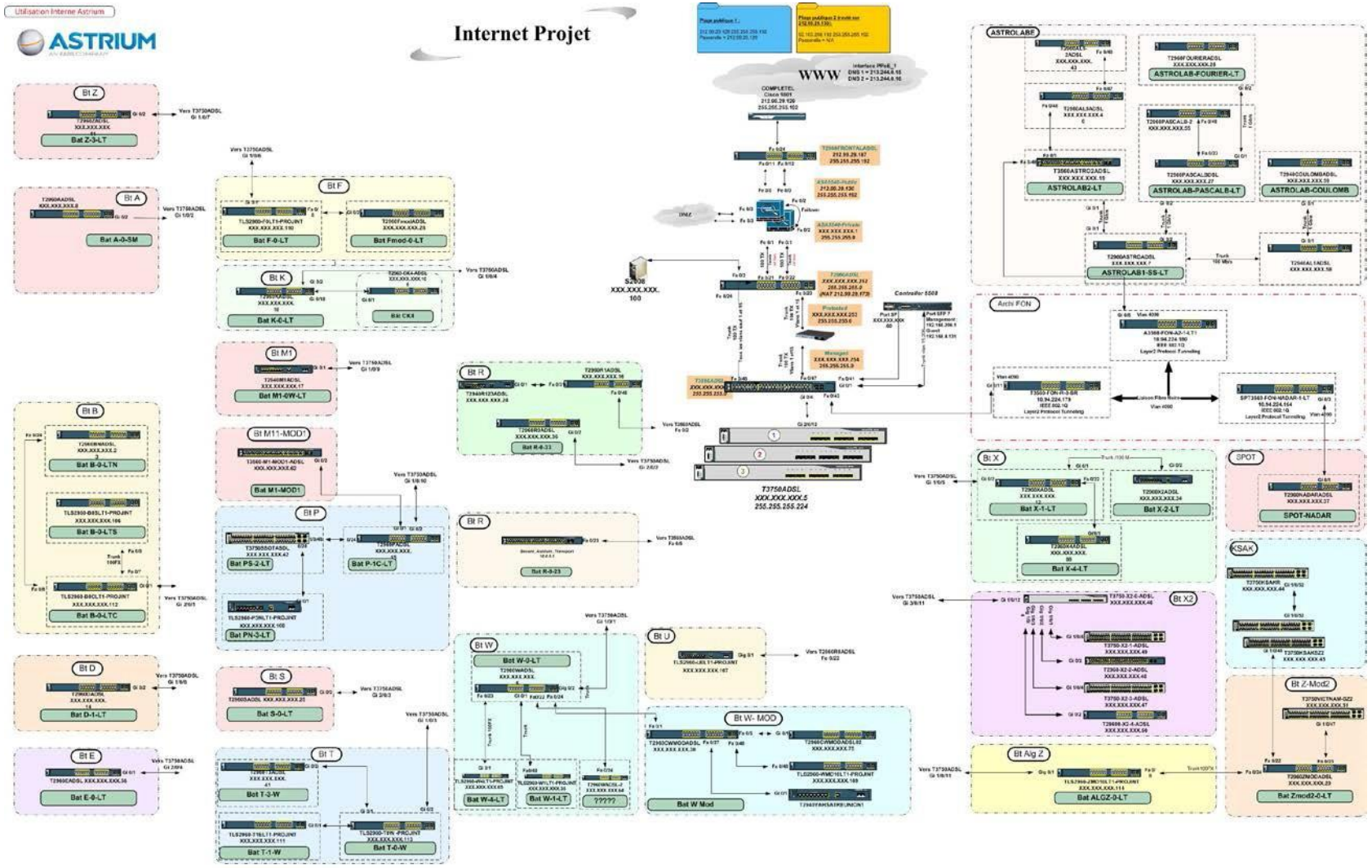


Figure 15 : Ancien schéma représentant l'architecture à plat

III.1 PHASE PREPARATOIRE

Avant de démarrer les phases techniques concernant l'usage et la configuration des protocoles et atteindre la cible que l'on s'est fixée, il est important de connaître l'environnement de départ.

III.1.1 DEFINITION DU PERIMETRE

III.1.1.1 ARCHITECTURE

III.1.1.1.1 ARCHITECTURE GENERALE

La Figure 15 ci-contre représente le schéma à partir duquel l'étude à démarré. Il s'agit d'un réseau en étoile, dont le cœur, constitué du plusieurs switches (3750 et 3560), se situe dans un bâtiment spécifique. Les switches de distribution sont positionnés directement dans les bâtiments et cascadés les uns derrière les autres en cas de sous-dimensionnement.

III.1.1.1.2 ARCHITECTURE PHYSIQUE

- ***Accès***

Les utilisateurs sont reliés aux switches d'accès à 100 Mbps par des câbles cuivre. Eux-mêmes sont cascadés derrière des switches de distribution[17].

- ***Accès distants***

Les sites distants sont raccordés via des liaisons spécialisés mono raccordées sur un même équipement en câble cuivre à 10 Mbps. Les sites toulousains sont raccordés via une fibre noire à 1 Gbps.

- ***Distribution***

Les switches sont, pour la plupart[18], raccordés au cœur de réseau par l'intermédiaire de rocades fibres optiques à 1 Gbps.

- ***Internet***

L'accès à Internet se fait au travers d'un routeur opérateur Completel. Une bande passante de 40 Mbps est allouée au trafic d'Astrium.

[17] Ces switches sont communément appelés switches de pied de bâtiments.
[18] Le patron de l'inventaire est disponible en Annexe 6

III.1.1.1.3 ARCHITECTURE LOGIQUE

Ici sont décrites les principales spécificités liées de près ou de loin à l'architecture de départ. Ceci afin de nous permettre d'ajuster au mieux les choix qui seront faits en matière de refonte de l'architecture, mais aussi et surtout dans les choix des protocoles.

Le réseau Internet Projet s'est construit sur la base d'un LAN. Les premières extensions du réseau qui ont été réalisées concernaient des bâtiments et le choix qui a été fait à ce moment fut de rester sur une architecture de niveau 2, sous-entendu sans routage.

- ***QinQ***

Par la suite, d'autres extensions sont apparues, leur raccordement nécessitant l'intervention d'un opérateur (MAN), certains mécanismes ont dû être mis en place pour pouvoir conserver ce mode non routé : le QinQ[19]. Ainsi les vlans peuvent transiter au travers du lien opérateur.

- ***VLANs***

À chaque projet manifestant le besoin d'accéder à Internet, est attribué un VLAN. Ces vlans sont indépendants les uns des autres. Les personnes travaillant sur ces projets étant mobiles sur tout le site, un serveur VTP est configuré pour distribuer de façon automatique les informations à tous[20] les switches.

- ***Spanning-tree***

Le spanning-tree est géré de façon automatique, avec la configuration par défaut sur tous les équipements. Le mécanisme de storm-control[21] est activé par défaut et la configuration par défaut répond aux besoins courants.

III.1.1.2 SERVICES

- ***Guest access***

Un vlan particulier est dédié aux guest access[22] afin de permettre aux personnes de passage d'avoir un accès limité à Internet (sous réserve d'avoir obtenu un compte temporaire).

- ***WiFi***

Une solution de WiFi guest access est à l'étude, mais reste à l'état de POC[23]. Elle est tout de même intégrée dans le réseau et est à prendre en compte lors des migrations.

---

[19] Le détail du fonctionnement est disponible en Annexe 4
[20] Tous les switches appartenant au même domaine. Les détails techniques ne sont pas abordés ici.
[21] Protection contre les tempêtes de broadcast, notamment utile lors de la détection d'une boucle sur le réseau.
[22] Accès invité, voir glossaire.
[23] Proof Of Concept. Maquette servant à démontrer l'utilité ou la faisabilité technique d'une solution.

- ***VPN IPSEC***

Les partenaires industriels, ou les clients nécessitant de communiquer de façon sécurisée utilisent des liaisons VPN IPSEC. Cela représente environ une quinzaine de VPN actifs.

- ***Filtrage***

Les accès internet entrants et sortant sont analysés, filtrés et journalisés. De même, le routage et/ou filtrage inter Vlan le cas échéant.

III.1.1.3 EQUIPEMENTS

- ***Switches Cisco***

Les switches 2940, 2950 et 2960 sont positionnés sur les couches accès et distribution.

Les switches 3750 sont en position de cœur de réseau et sont censés être root bridge[24].

Le switch 3560 sert principalement à fédérer les accès distants et fait office de serveur VTP.

- ***Routeur Cisco***

Le routeur 1801 est un routeur mis à disposition et géré par l'opérateur Internet.

- ***Serveurs Cisco ASA***

Deux serveurs ASA 5510 (en failover[25]) localisés dans une même baie servent à la fois de passerelle, de firewall et de concentrateur VPN. C'est également eux qui gère l'étanchéité entre les VLAN.

- ***Contrôleur BlueSocket***

Cet équipement sert à la gestion des guest access. Son rôle est très important, car il est positionné en coupure du réseau d'administration et de celui du guest.

- ***Contrôleur Cisco WLC***

Dans le cadre de la maquette (non en production), il sert à administrer et superviser les points d'accès du réseau Wifi de manière centralisée.

- ***Serveur Windows 2008 Server***

Ce serveur héberge les différents services et logiciels utiles à l'administration et la supervision du réseau Internet Projet.

[24] La notion de root brigde sera abordée plus loin avec le concept de spanning-tree.
[25] Protocole de redondance qui sera abordé plus loin.

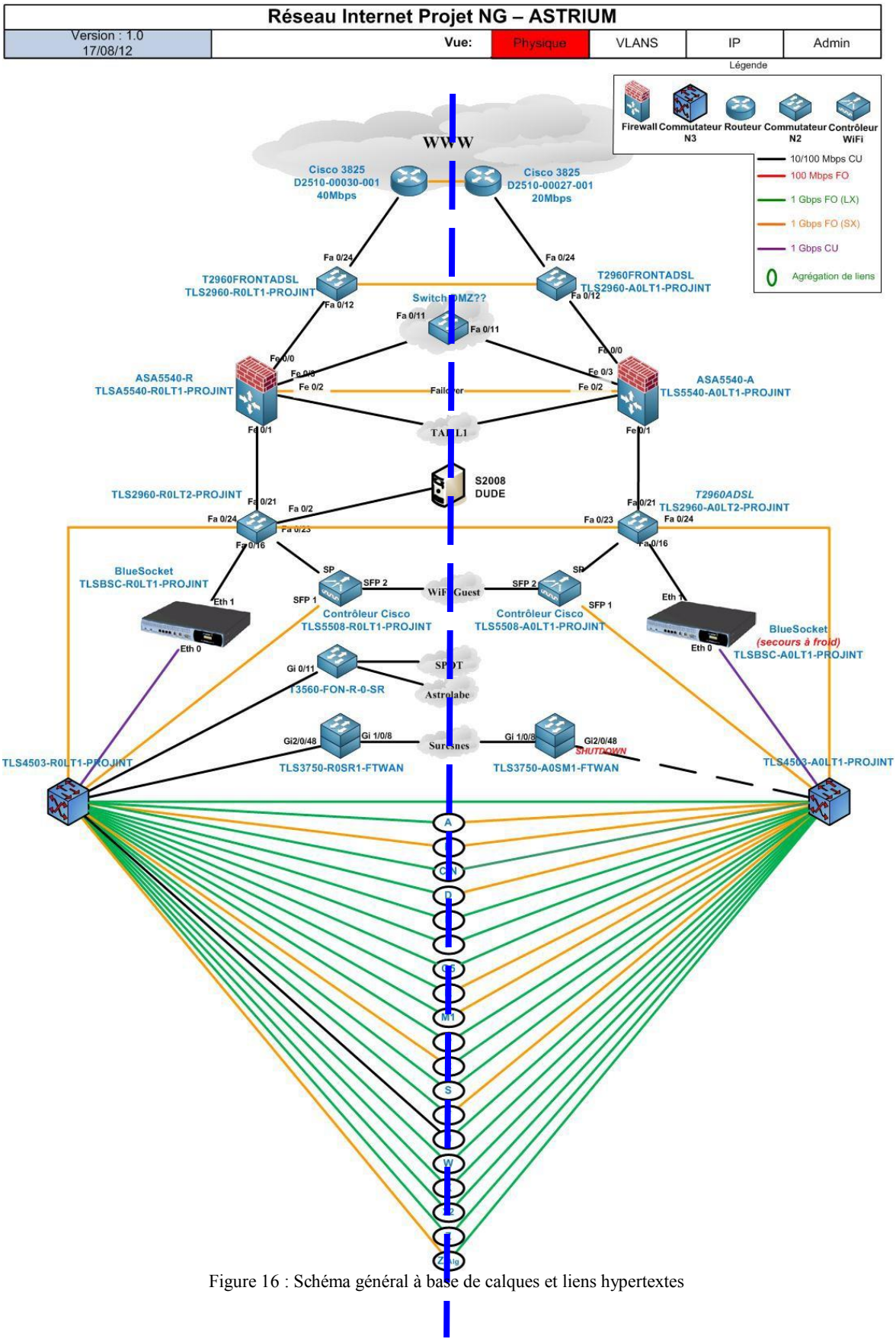


Figure 16 : Schéma général à base de calques et liens hypertextes

III.1.2 DEFINITION DE LA CIBLE

III.1.2.1 ARCHITECTURE

III.1.2.1.1 ARCHITECTURE GENERALE

La **Erreur ! Source du renvoi introuvable.** ci-contre représente le nouveau schéma[26] qui a été construit et qui sert dorénavant de référence. Il s'agit d'un document Visio qui s'appuie sur la superposition de différents calques[27] pour pouvoir afficher successivement les informations physique (type de câblage, port, et vitesse), celles de niveau 2 (VLAN, STP), puis d'adressage IP et enfin l'adressage d'administration.

Sur celui-ci, on voit clairement une symétrie de part et d'autre de l'axe matérialisé par les pointillés bleus. A droite figurent les équipements actuellement existant dans un bâtiment que nous appellerons A. Agauche, les équipements qui seront positionnés dans un autre bâtiment, que nous appellerons B.

Sur l'axe central sont positionnés tous les équipements qui seront double-attachés. On y distingue, les accès distants (au centre), le DMZ ainsi que des liens vers l'ensemble des bâtiments[28] (dans le « triangle » du bas)

III.1.2.1.2 ARCHITECTURE PHYSIQUE

- ***Accès***

Les utilisateurs seront toujours reliés aux switches d'accès à 100 Mbps par des câbles cuivre. Eux-mêmes sont cascadés derrière des switches de distribution[29] sur des liens fibres à 1 Gbps.

- ***Accès distants***

Les sites distants sont double-raccordés sur les cœurs de réseaux via des liaisons spécialisées lorsque cela est possible, c'est à dire, lorsque le site est assez important pour investir sur l'installation d'une deuxième ligne opérateur. Dans le cas où cela ne se justifie pas, on conserve un lien unique mono raccordé sur un même équipement en câble cuivre à 10 Mbps. Les sites Toulousains sont raccordés via une fibre noire à 1 Gbps. Une deuxième liaison est en cours de commande et ne figure pas sur ce schéma.

[26] Des copies d'écran sont disponibles en Annexe 2
[27] Des copies d'écran ainsi que le script permettant les changements de calques sont disponibles en Annexe 3.
[28] Il s'agit de liens hypertextes qui renvoient vers un autre onglet du même document.
[29] Ces switches sont communément appelés switches de pied de bâtiments.

- ***Distribution***

Les switches sont tous raccordés aux deux cœurs de réseau par l'intermédiaire de rocades fibres optiques à 1 Gbps.

- ***Cœur de réseau***

Deux cœur de réseau équipés de carte fibre au gigabit permettent de double raccorder l'ensemble des éléments du réseau Internet Projet.

- ***Internet***

L'accès à Internet se fait au travers de deux routeurs opérateur Completel redondant[30] l'un de l'autre. Une bande passante de 40 Mbps est allouée au trafic d'Astrium, aussi bien sur l'accès primaire que sur le secondaire.

III.1.2.1.3 ARCHITECTURE LOGIQUE

En prenant en compte les principales spécificités liées à l'architecture de départ, nous avons effectué des choix en matière de refonte de l'architecture, mais aussi et surtout dans les choix des protocoles utilisés.

Pour rappel, le réseau Internet Projet s'est construit sur la base d'un LAN et le choix qui a été fait à la naissance du projet fut de rester sur une architecture de niveau 2. Aujourd'hui, les besoins évoluant, il est question de changer cela pour s'orienter dans un futur proche (courant 2013), vers un mode routé. Aussi, nous avons dû intégrer ce paramètre dans notre analyse afin que le présent document puisse servir de base à la mise en place du routage.

- ***QinQ***

En attendant que l'on puisse faire du routage entre les différents sites, le protocole 802.1ad (QinQ) est conservé. Toutefois des mesures ont été prises afin de rendre possible la migration en mode routé qui devrait avoir lieu courant 2013.

- ***VLANs***

Le mode de création des VLANs ne change pas, hormis le fait qu'un second serveur VTP[31] est configuré pour assurer le backup en cas de défaillance du premier.

- ***Spanning-tree***

Le spanning-tree qui était géré de façon automatique est maintenant configuré manuellement[32] afin d'en maitriser davantage le fonctionnement. Le mécanisme de storm-control a été ajusté pour répondre davantage aux cas concrets de boucles sur le réseau.

---

[30] La description des mécanismes est disponible là
[31] La description des mécanismes est ici
[32] Une description détaillée est proposée ici

III.1.2.2 SERVICES

- ***Guest access, WiFi, VPN IPSEC et filtrage***

Ces 3 services, bien qu'inchangés sont soumis aux mêmes modifications, à savoir un double attachement aux chaînes nominales et secours.

III.1.2.3 EQUIPEMENTS

Les équipements EOL/EOS[33] ont été remplacés afin d'obtenir un parc plus homogène, en facilité l'administration, le support et la maintenance.

- ***Switches Cisco***

Des switches 2960 et 2960S viennent remplacer les 2940, 2950 et sont positionnés sur les couches accès et distribution.

Deux châssis 4500 prennent la place des switches 3750 en position de cœur de réseau et sont configurés en root bridge, ainsi qu'en serveur VTP. Ils sont positionnés dans les bâtiments A et B.

- ***Routeurs Cisco***

Deux routeurs 1801 sont mis à disposition et gérés par l'opérateur Internet. Ils sont positionnés dans les bâtiments A et B.

- ***Serveurs Cisco ASA***

Deux serveurs ASA 5510 servent à la fois de passerelle, de firewall et de concentrateur VPN. Ils sont positionnés dans les bâtiments A et B.

- ***Contrôleurs BlueSocket et Cisco WLC***

Un deuxième équipement (anciennement « sur étagère ») est venu en complément[34] de chacun des équipements. Ces équipements seront positionnés au bâtiment B.

- ***Serveur Windows 2008 Server***

Aucun changement hardware pour ce serveur, même si des mécanismes[35] de sauvegarde ont été implémentés pour prévenir des pannes.

---

[33] End Of Life/End Of Sale. Fin de fin et de vente.
[34] Le mécanisme de redondance sera détaillé plus loin
[35] Les différentes solutions proposées sont là

III.1.3 PRE REQUIS

Avant de pouvoir entrer dans le vif du sujet et retrouver notre problématique de départ, il est important de mesurer l'importance des étapes préparatoires. Aussi, cette partie a pour but de répertorier les étapes qui ont été effectuées avant de pouvoir commencer à travailler sur les aspects plus techniques.

III.1.3.1 LOCAUX TECHNIQUES

Afin de pouvoir installer les équipements commandés dans le bâtiment B, il faut au préalable identifier et réserver un emplacement adéquat dans lequel ils pourront être installés. Pour ce faire, nous avons estimé le volume de chaque équipement ainsi que le nombre de U[36] nécessaire, pour pouvoir déterminer le nombre et le type de baies dont nous avions besoin. Une fois cette étape réalisée, nous avons obtenu une certaine surface en m² qui nous a permis de demander que ce nombre de m² supplémentaires soit alloué au projet pour pouvoir y installer nos baies.

III.1.3.2 ALIMENTATION ELECTRIQUE

Une fois les surfaces réservées et les baies montées, l'alimentation électrique peut être installée. Deux arrivées, provenant de deux circuits différents existent sur le site.

Aussi, il est important de sélectionner une arrivée différente de celle du bâtiment A (ce qui est déjà le cas par défaut). Ensuite viennent se positionner les onduleurs pouvant alimenter l'ensemble des équipements pendant une courte durée en cas de défaillance du système électrique. Puis enfin, les équipements que l'on installe dans la baie et que l'on raccorde sur ces onduleurs. À noter qu'en cas de double-alimentation, chacune est installée sur un bloc différent afin de conserver cette même logique de redondance.

Ces locaux sont gérés par les moyens sites, une fois les informations nécessaires fournies, ils se sont chargés du calcul de la puissance électrique utile ainsi que de la nécessité d'adapter le système de refroidissement des salles ou non.

[36] Unité de mesure utilisée dans les baies télécoms pour indiquer la hauteur d'un équipement, 1U = 4,5 cm.

III.1.3.3 CABLAGE

Maintenant que le matériel est en place (éteint pour éviter tout problème avant que tout ne soit correctement configuré), il reste à le raccorder au réseau de production. Pour se faire, il est indispensable de prévoir et de réserver des rocades fibres.

III.1.3.4 DOCUMENTATION

Avant de pouvoir démarrer, il est important de documenter chacune des étapes, dans un plan de migration, de mettre à jour les documents existants. Afin de garantir le bon suivi du projet, des livrables sont à prévoir. En l'occurrence, un dossier d'architecture ainsi qu'un dossier d'exploitation ont été élaborés. Ces documents sont aujourd'hui utilisés par l'équipe d'exploitation. Par ailleurs, une présentation des fonctionnalités utilisées sous Visio a également été dispensée.

III.1.3.5 COMMUNICATION

Un autre aspect important de cette étape de pré requis concerne la communication. Qu'il s'agisse de planifier un créneau d'intervention avec les équipes opérationnelles, les opérateurs internet, ou encore les utilisateurs finaux, de présenter un plan de migration pour le faire valider, ou encore d'effectuer un transfert de compétences sur la solution mise en place : la communication est présente au quotidien et elle doit être intégrée dans la gestion du projet.

III.1.3.6 VERSIONS

Enfin, l'ensemble des versions a été relevé et comparé avec les versions plus récentes afin de maitriser l'état du parc que ce soit d'un point de vue matériel ou logiciel. Lors de cet inventaire, il est apparu que la plupart des versions étaient obsolètes[37]. Le remplacement d'une bonne partie du parc a permis de corriger une partie. Une analyse plus précise a été nécessaire afin de déterminer s'il était nécessaire de mettre à jour le parc en fonction des protocoles à utiliser. Il s'est avéré que certaines fonctionnalités basiques[38] nécessitaient tout de même une mise à jour. Aussi, il a été décidé d'upgrader le parc complet de switches. Ceci a été très consommateur de temps puisqu'il a fallu coordonner les actions avec les différents responsables de projets en période de congés estivaux.

[37] Tableau d'inventaire disponible en Annexe 6
[38] Certaines options de spanning-tree ainsi que le SSH n'étaient pas supporté par la plupart des équipements.

III.2 DISTRIBUTION

III.2.1 DEFINITION DU BESOIN

III.2.1.1 RAPPEL DU CONTEXTE

Le plan d'action, issue de l'analyse de risque du plan de continuité d'activité, traite de la suppression des points de panne unique (SPOF). Ainsi, nous avons vu dans la partie précédente comment les switches de distribution sont double-attachés aux deux cœurs de réseau. La mise en place de liens résilients entre la couche distribution et la couche core permet d'offrir un ou plusieurs chemins d'accès alternatifs en cas de panne d'un commutateur. Cependant à ce stade, le cœur de réseau du bâtiment B (site secours) n'est toujours pas alimenté afin de ne pas créer de boucle de niveau 2 sur le réseau.

III.2.1.2 OBJECTIF

Une telle architecture implique en effet la création de boucle sur le réseau informatique. Ces boucles provoquent des tempêtes de diffusion[39] qui inondent les tables d'apprentissage des équipements et entrainent l'écroulement du système. L'objectif est donc de pouvoir conserver la résilience des liens sans paralyser le réseau.

Une solution simple consisterait à désactiver le port allant vers le cœur de réseau du bâtiment B et à l'activer manuellement lorsqu'une panne sur l'autre lien est détectée[40].

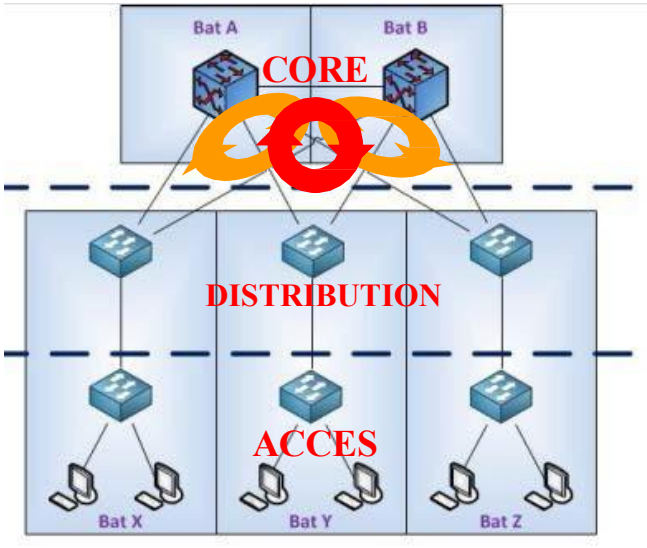


Figure 17 : Boucles de niveau 2 entre les couches

Le Spanning-tree a été conçu pour répondre à cette problématique et permettre de réaliser des architectures offrant de la redondance.

[39] Broadcast storm
[40] Ceci impliquerait de désactiver l'interface du lien défectueux afin d'éviter la création une nouvelle boucle.

III.2.2 LE SPANNING-TREE

III.2.2.1 PRINCIPE DE FONCTIONNEMENT

Dans sa conception intrinsèque, Ethernet impose une topologie sans boucle, et par conséquent oblige à l''unicité du chemin entre deux équipements. En cas de création d'une boucle, les trames de types broadcast « tournent en rond » sans qu'elles puissent être supprimées[41]. Le principe général du Spanning-tree consiste à garantir un chemin logique unique entre deux points et de bloquer intentionnellement les ports responsables des boucles sur le réseau.

Pour se faire, l'ensemble des commutateurs configurés pour utiliser STP échange régulièrement (toutes les deux secondes) des trames particulières appelées BPDU (*Bridge Protocol Data Units*). Ces trames, qui contiennent des informations comme le BID (Bridge Identifier), mais aussi des indications de configuration ou de changement de topologie, permettent à tous les commutateurs de connaître la topologie du réseau à un instant « T ».

III.2.2.1.1 ELECTION DU ROOT BRIDGE[42]

Le protocole Spanning-tree s'appuie sur un algorithme pour déterminer un chemin unique. Pour cela, il doit désigner un commutateur unique comme pont racine (root bridge) qu'il utilisera comme point de départ de tous ses calculs. À chaque commutateur est affectée une priorité paramétrable (0x8000 par défaut), associée à son adresse MAC, elles constituent l'identifiant de pont (*bridge identifier*, BID). Le commutateur avec la priorité la plus basse est élu roort bridge. Lorsque les priorités sont laissées par défaut (elles sont donc toutes identiques), c'est sur l'adresse MAC que repose l'élection, et c'est celui qui a la plus petite qui l'emporte.

III.2.2.1.2 CALCUL DU SHORTEST PATH[43]

Une fois l'élection du root bridge effectuée, les autres commutateurs vont alors calculer la distance plus courte vers la racine. Le coût de chemin est calculé à l'aide de la valeur de la somme des coûts des liens (qui dépend de sa bande passante port de chacun des ports des commutateurs) pour un chemin donné.

---

[41] Il n'y a pas de TTL comme sur IP, et les mécanismes existant pour les filtrer sont gourmands en ressource.
[42] Pont racine
[43] Chemin le plus court

III.2.2.1.3 DETERMINATION DES ROOT PORTS[44]

Chaque commutateur non-root, va affecter un port Root qui sera sur le chemin le plus court vers le switch Root. L'élection d'un root port est effectuée d'après les champs path cost et port ID d'un paquet BPDU. Il ne peut y avoir qu'un seul root port par commutateur. Dans le cas où les coûts seraient identiques, c'est la priorité la plus faible (entre 0 et 255) qui détermine le choix. Cette priorité (128 par défaut) est obtenue en additionnant l'ID du port (sur 2 octets) à la priorité STP.

III.2.2.1.4 DETERMINATION DES DESIGNATED PORTS[45]

Pour chaque segment réseau (domaine de broadcast) reliant des commutateurs, le designated port est celui qui a le chemin le plus court vers le bridge Root. Dans le cas où les coûts seraient identiques, c'est la priorité la plus faible (entre 0 et 255) qui détermine le choix. Cette priorité (128 par défaut) est obtenue en additionnant l'ID du port (sur 2 octets) à la priorité STP.

III.2.2.2 FOCUS SUR LES PORTS

III.2.2.2.1 LES ROLES

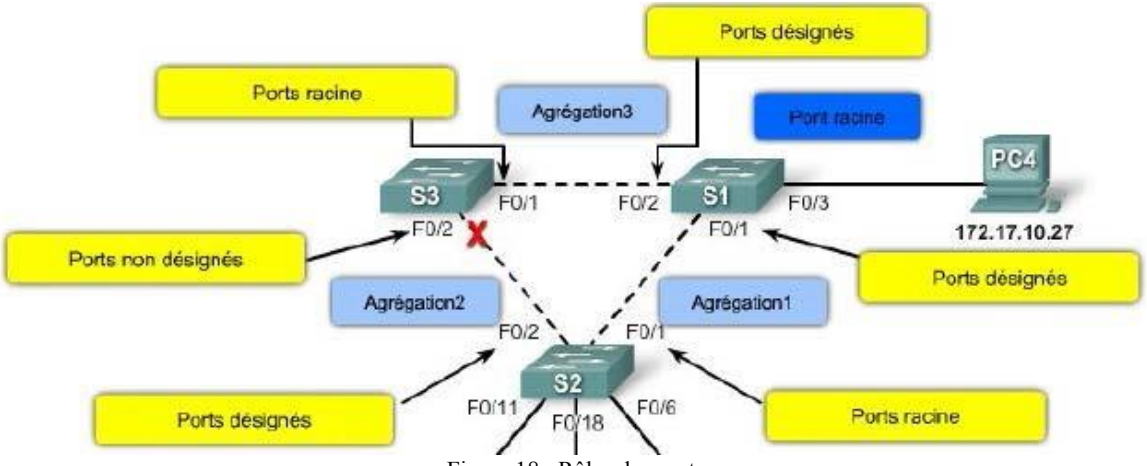


Figure 18 : Rôles des ports

- 1 Root bridge par réseau dont tous les ports sont « designated port ».
- 1 Root port par commutateur (excepté le Root Bridge).
- 1 Designated port par domaine de broadcast.
- Tous les autres ports sont configurés en « non-désignated port ».

[44] Ports racine
[45] Ports désignés

III.2.2.2.2 LES ETATS[46]

Le port d'un commutateur, avec le spanning-tree est activé, peut prendre 5 états différents pendant le processus de construction de la topologie de niveau 2.

- **Listening :** mode « écoute » pour déterminer la topologie courante (grâce aux BPDU).
- **Learning :** construction d'une table de forwarding en associant les adresses MAC aux ports.
- **Forwarding :** Réception et envoi de paquets.
- **Blocking :** Blocage du port (détection d'une boucle), aucun envoi ou réception de données.
- **Disabled** : désactivation manuelle (action de l'administrateur)

Le tableau ci-dessous récapitule à quoi correspond chaque état.

Tableau II : Représentation des états des ports

Processus	Blocking	Listenning	Learning	Forwarding	Disabled
Réception et traitement des trames BPDU	*OUI	OUI	OUI	OUI	NON
Acheminement des trames de données reçues sur l'interface	NON	NON	NON	OUI	NON
Acheminement des trames de données commutées depuis une autre interface	NON	NON	NON	OUI	NON
Apprentissage des adresses MAC	NON	NON	OUI	OUI	NON

Lorsqu'un équipement est connecté sur un port, celui-ci passe successivement des états Listenning à learning, puis à Forwarding). Ce délai est appelé forward delay et prend 15 secondes par défaut. Afin de raccourcir ce délai, le Rapid STP (802.1w) permet au port d'un commutateur de passer directement en mode forwarding. Dans notre cas, nous utiliserons la fonction de portfast proposée par Cisco et appliquée à tous les ports d'accès.

[46] Les états des ports sont détaillés en Annexe 7

III.2.2.3 CAS CONCRET

III.2.2.3.1 ROOT BRIDGE

Les deux figures ci-dessous illustrent le comportement attendu dan la configuration effectuée chez Astrium.

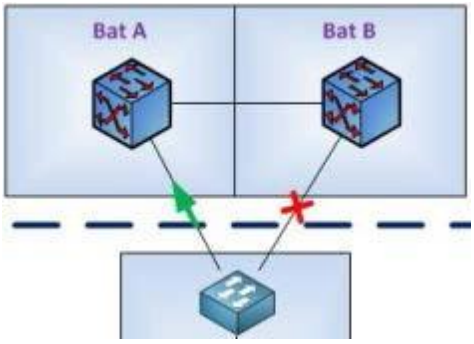


Figure 19 : STP en configuration nominale

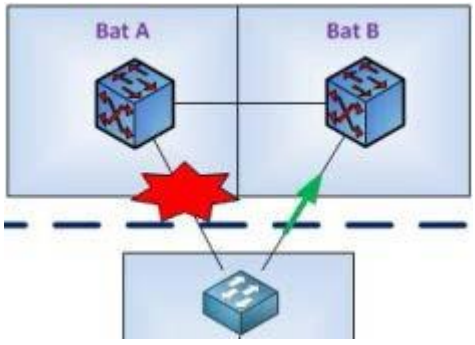


Figure 20 : Défaillance sur le lien nominale

Des commandes Cisco permettant de forcer un équipement en Root Bridge Primaire ou secondaire existe, mais nous avons préférer positionner manuellement ces valeurs. Le cœur de réseau A est donc configuré en Root Bridge, sa priorité a été modifiée manuellement. La priorité de celui positionné en B est configurée pour qu'il soit automatiquement élu Root Bridge en cas de défaillance du premier.

III.2.2.3.2 SHORTEST PATH

L'ensemble des couts des liens a été analysé afin de vérifier qu'en mode nominal, le chemin le plus court emprunter pour accéder à Internet transitait exclusivement par les équipements situés au bâtiment A. Aucune adaptatation particulière n'a été apportée à la configuration initiale.

III.2.2.3.3 VALIDATION

Différents scenarios ont été testés et sont détaillés en Annexe 8. Ceux-ci ont permis de valider le fonctionnement correct du spanning-tree. Ainsi tous les switches de distributions sont maintenant double-attachés et la redondance assurée.

- ***Quelques commandes de vérifications***

switch#show spanning-tree root
switch#show spanning-tree summary
switch#show spanning-tree detail
switch#show spanning-tree blockedports

III.3 CŒUR DE RÉSEAU

III.3.1 DEFINITION DU BESOIN

III.3.1.1 RAPPEL DU CONTEXTE

Le plan d'action issue du plan de continuité d'activité traite de la suppression des points de panne unique (SPOF). Le remplacement de la pile de switches 3750 par deux châssis Cisco 4500, nous permet de redessiner les bases de cette architecture. À noter qu'au moment de notre étude, le VSS (Virtual Switching System) n'est pas encore disponible sur ces types d'équipements (sortie prévue en Décembre 2012). Hormis les caractéristiques propres à l'équipement (double alimentation Hot swappable[47], et NSF[48]). La redondance entre les deux équipements réside donc uniquement dans le paramétrage de leur priorité STP qui leur confère les rôles de Primary et Secondary Root-Bridge. Ainsi, nous avons vu dans la partie précédente comment le protocole Spanning-tree permet aux switches de distribution d'être raccordés à ces cœurs de réseau avec un lien actif et l'autre passif.

III.3.1.2 OBJECTIF

La conception actuelle du réseau s'appuie sur une architecture de niveau 2, mais va prochainement évoluer vers du niveau 3 (routé). Ceci nous permettra de mieux desservir les sites distants et de s'affranchir de certaines contraintes liées à la mutualisation de certains accès opérateur (utilisation du QinQ), mais aussi de limiter les échanges de protocoles de niveau 2 (Spanning-tree, CDP) au travers de liens WAN. L'objectif est donc de proposer une solution redondante s'appuyant sur l'utilisation de protocole de niveau 3.

III.3.2 LE ROUTAGE

Le routage est aujourd'hui assuré par les serveurs Cisco ASA. Le contenu de la partie suivante reste donc purement théorique et a pour objectif de présenter les avantages d'un réseau routé.

De plus, les protocoles de routage dynamiques ne seront pas abordés ici. En effet, concernant ceux à vecteur de distance leur principale limitation réside dans le fait que leurs calculs de distance s'appuient nombre de sauts (limité à 15) entre deux points.

[47] Échangeable à chaud. Sans coupure électrique.
[48] Non Stop Forwarding. Haute disponibilité des cartes supervisor intra-chassis.

La bande passante ou l'état d'un lien ne sont pas pris en compte alors qu'ils le sont avec les protocoles à état de lien.

Le besoin en termes de routage concerne uniquement les sites distants puisqu'il n'y a pas de communication inter-vlan. L'utilisation des protocoles à état de lien ne se justifie pas non plus et l'on pourra se contenter de quelque route statique agrémentée d'une route flottante le cas échéant pour assurer le backup.

III.3.2.1 VSS EN COMPLEMENT

Cette solution n'étant pas encore applicable à notre projet, nous n'abordons ici que le concept général.

VSS n'est pas un protocole, mais plutôt une technologie de niveau 2 développée par Cisco, qui permet de s'affranchir des contraintes souvent rencontrées sur les réseaux de Campus, liées à l'utilisation du Spanning-tree. L'avantage principal est donc de pouvoir se passer dû STP entre les couches d'accès et de cœur. Le temps de convergence est donc fortement amélioré. Virtual Switching System permet de construire un cluster d'au moins deux châssis (Sur les modèles 6500 uniquement pour l'instant) pour en faire une seule entité virtuelle. Ce système apporte ainsi des améliorations notables en matière vitesse de commutation, d'architecture, de haute disponibilité, et d'évolutivité.

Par ailleurs, il permettrait également de s'affranchir des fonctions de redondance de la passerelle (type HSRP). En effet, l'adresse de passerelles des machines raccordées au réseau sera gérée par l'ensemble du système VSS.

III.4 ACCÈS INTERNET

III.4.1 DEFINITION DU BESOIN

III.4.1.1 RAPPEL DU CONTEXTE

Le premier évènement déclencheur de la construction du plan de continuité d'activité fut la coupure de l'accès Internet. Le plan d'action issu de ce PCA traite de la suppression des points de panne unique (SPOF) et la redondance de cet accès à internet est une priorité pour le management. Aussi, des réunions ont été rapidement montées avec l'opérateur afin de trouver ensemble une solution à ce genre de problématique pour qu'elle ne se reproduise pas.

III.4.1.2 OBJECTIF

Un PoP[49] différent situé à proximité du site client a permis l'acheminement d'un deuxième accès Internet. S'il avait été question de deux opérateurs différents, nous aurions pu nous contenter de la configuration d'une route par défaut, et d'une route de backup pointant sur chacun des équipements mis à notre disposition. Cependant, s'agissant du même opérateur, il était intéressant de pouvoir conserver l'usage d'une passerelle unique. L'objectif est donc de pouvoir pointer sur une passerelle unique et d'obtenir de la redondance entre les deux accès internet.

III.4.2 LE HSRP

Bien que les équipements soient sous maitrise opérateur, nous avons pu obtenir certaines informations de configurations concernant les méthodes et protocoles utilisés pour assurer cette redondance. Notamment concernant l'utilisation et la configuration du HSRP.

Hot Standby Router Protocol (HSRP définit par la RFC 2281) est un protocole propriétaire de Cisco qui permet d'assurer une continuité de service en cas de panne ou d'indisponibilité de la passerelle par défaut d'un réseau.

[49] Point Of Presence

III.4.2.1 PRINCIPE DE FONCTIONNEMENT

HSRP est décrit dans la RFC 2281.C'est FHRP (First Hop Redundancy Protocol) propriétaire Cisco semblable au VRRP qui permet de sécuriser une passerelle IP assurant une haute disponibilité.

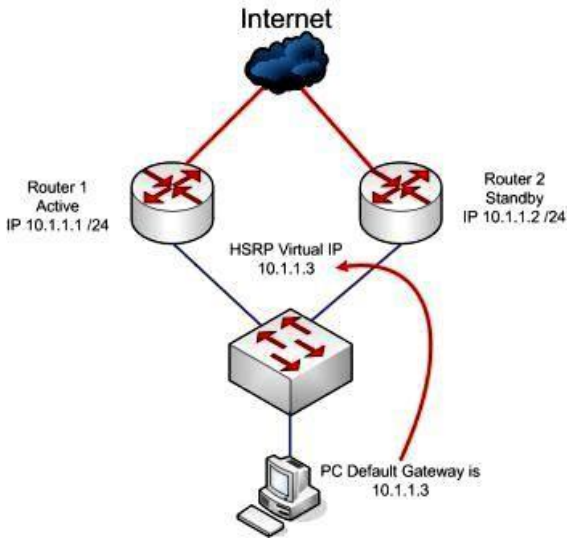


Figure 21: Principe du HSRP

Une adresse IP virtuelle associée à une adresse MAC également virtuelle est partagée par (au moins) deux équipements de niveau 3. Ces routeurs élisent un routeur maitre, c'est-à-dire celui qui portera l'adresse à un instant « T ». Celui qui a la priorité la plus haute passera donc en statut « actif » et répondra aux requêtes envoyées à l'IP virtuelle du groupe HSRP. Du point de vue de l'utilisateur, bien qu'elle corresponde à plusieurs équipements, une seule passerelle est visible.

En cas de défaillance du routeur maitre (actif), l'un des équipements du groupe (celui qui aura la priorité la plus haute) passera du mode standby[50] au mode actif et prendra le rôle du master en portant l'adresse IP/MAC du groupe.

[50] attente

III.4.2.1.1 ELECTION DU MASTER

Les messages HSRP utilisent l'adresse multicast 224.0.0.2 sur port UDP 1985.

Le mode de communication est unilatéral, seul le routeur master envoie des Hello paquets aux routeurs standby (toutes les 3s) pour les informer de son état (actif).

Un hold time est fixé afin que tous les équipements en standby puissent avoir connaissance de la fenêtre pendant laquelle ils sont censés recevoir un message « Hello » du routeur actif. En cas de défaillance du primaire, ce délai arrive à expiration, et ils procèdent à une réélection. Le nouveau routeur primaire qui est élu est celui de plus forte priorité (valeur comprise entre 1 et 255, 100 par défaut). À noter qu'à priorité égale, c'est le routeur ayant la plus grande adresse IP qui remportera l'élection.

III.4.2.1.2 SURVEILLANCE RESEAU

Le protocole HSRP permet de surveiller uniquement l'état d'un équipement. En revanche, un problème sur une interface ou sur un équipement distant est indétectable. Afin de pallier ce manque, il est possible, voire nécessaire de configurer le routeur pour qu'il supervise l'état d'une interface ou la présence d'une route dans sa table de routage. On augmente ainsi la granularité d'analyse et la finesse de bascule en cas de défaillance de l'équipement primaire. Lorsque l'état n'est pas conforme, la priorité est décrémentée. La fonction « preempt » permet alors à l'un des équipements « standby » de prendre la main.

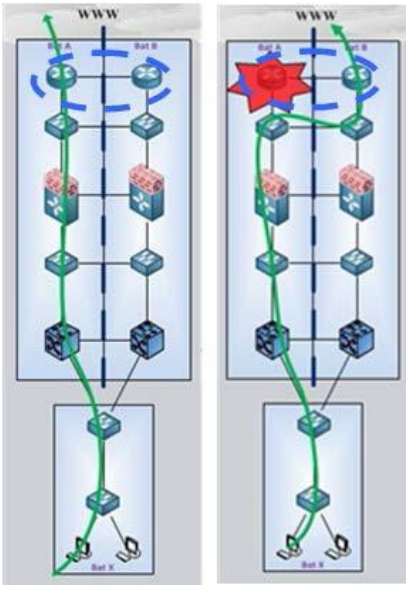


Figure 22: Défaillance du routeur nominal

III.4.2.2 VALIDATION

Les deux routeurs d'accès Internet sont raccordés sur deux PoP différents dont les extrémités se situent dans les bâtiments A et B. Avant l'ajout du second routeur, le premier a été configuré en HSRP. Son adresse réelle a été libérée pour pouvoir être utilisée par l'adresse virtuelle du groupe HSRP. Une fois les configurations prêtes, les deux équipements ont été mis sous tension et des tests de bascule ont été réalisé (schéma de droite dans l'Annexe 8) pour valider le transfert de l'adresse IP et MAC vers le bon routeur.

Une fois le problème de rafraichissement de table arp sur un switch défaillant résolu, les tests ont été concluants.

- ***Quelques commandes***

```
Router(config)#interface Vlan2
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#standby 8 ip 10.0.0.254
Router(config-if)#standby 8 priority 110
Router(config-if)#standby 8 preempt
Router1(config)#track 1 ip route 128.4.128.8 255.255.255.0 reachability
Router1#show standby brief
```

III.5 APPLICATION (RESEAU)

III.5.1 DEFINITION DU BESOIN

III.5.1.1 RAPPEL DU CONTEXTE

Dans notre méthodologie nous avons présenté les protocoles utilisés pour effectuer de la redondance et donc supprimer les SPOF au niveau des différentes couches du réseau. Certains équipements ne rentrent pas dans ces catégories et apportent un service supplémentaire au niveau du LAN. Dans le cadre de ce projet, nous avons regroupé les firewalls et les contrôleurs Wifi dans une même partie, car ils fournissent nativement une solution de redondance qui s'appuie sur le même principe de fonctionnement.

III.5.1.2 OBJECTIF

L'objectif est ici un peu différent des parties précédentes, puisqu'il ne s'agit pas de présenter un choix technique associé à un protocole, mais plutôt de décrire le fonctionnement du protocole qui sert de base à nombre de ces mécanismes et notamment celui du failover.

III.5.2 LE FAILOVER

III.5.2.1 PRINCIPE DE FONCTIONNEMENT

III.5.2.1.1 LE PROTOCOLE CARP

Le mécanisme de failover natif dans nos équipements s'appuie sur le protocole CARP, similaire à celui de hsrp ou de vrrp.

CARP signifie « *Common Address Redundancy Protocol* » est un protocole sécurisé et libre qui permet de faire de la redondance d'adresse IP sur un réseau. Un groupe (appelé groupe CARP) de machines partage une même adresse IP ainsi qu'une même adresse MAC. Les hôtes CARP répondent aux requêtes ARP pour l'adresse commune avec l'adresse MAC virtuelle, et les annonces CARP elles-mêmes sont envoyées avec cette même adresse source, ce qui permet de déterminer rapidement sur quel port du commutateur l'adresse MAC virtuelle est à un instant « T ».

L'hôte maître (les autres sont appelés esclaves) de l'adresse envoie régulièrement des messages d'informations CARP en multicast en utilisant le protocole CARP (protocole IP 112), et les hôtes de backup écoutent ces messages. En cas de non-réception de message, les hôtes de backup renvoie des messages d'information afin d'élire un nouveau maître. La fréquence des messages est paramétrable, et l'hôte qui annonce le plus souvent est le plus susceptible de devenir maître en cas de défaillance.

CARP est donc utile pour réaliser une redondance efficace. Seulement, dans le cas d'un équipement réseau (firewall par exemple), cela ne suffit pas à éviter une coupure de service. En effet, toutes les sessions actives seront perdues. Il faut donc un mécanisme supplémentaire pour permettre une synchronisation régulière de la configuration, mais aussi des tables de connexions.

III.5.2.1.2 LE PROTOCOLE PFSYNC

Pfsync diffuse entre les pare-feu des messages d'insertion, de mise à jour, et de suppression d'état. Chaque pare-feu envoie ces messages en multicast sur une interface spécifiée, en utilisant le protocole pfsync (protocole IP 240). Il écoute également sur cette interface les messages similaires provenant de ses voisins, et les importe dans la table d'état locale.

Pour des raisons des risques de sécurité, il est fortement recommandé d'utiliser un réseau (un câble croisé ou VLAN) dédié pour utiliser pfsync.

III.5.2.2 VALIDATION

Ainsi nous venons de voir le fonctionnement général du failover assimilable à la combinaison[51] des protocoles CARP et PFsync. Leur utilisation peut être consommatrice de ressource et il est important de correctement ajuster les paramètres de synchronisation lorsque c'est possible.

À titre d'illustration, le contrôleur Bluesocket, équipement souvent chargé au-delà de 80% de CPU ne supporte pas la mise en œuvre du failover. Sa charge CPU atteint 100% et il n'est plus capable ni d'envoyer correctement les messages à son voisin, ni de rendre le service pour lequel il est conçu. Son backup ne recevant pas de message fait valoir son droit de préemption, et les deux équipements sont actifs en même temps sans pour autant pouvoir fonctionner. Nous avons dû nous résoudre à désactiver le failover et à conserver le mode de backup à froid.

En revanche, concernant les firewalls et les autres contrôleurs WiFi, aucune anomalie n'a été relevée, et la redondance est bien assurée. Différents tests de bascules ont été réalisés afin d'en valider le fonctionnement.

- ***Quelques commandes***

ciscoasa(config)#failover lan unit primary
ciscoasa(config)#failover lan interface failoverlink Ethernet0/1
ciscoasa(config)#failover key *****
ciscoasa(config)#failover link failover Ethernet0/7
ciscoasa(config)#failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2

ciscoasa#show failover

[51] Le chronogramme d'un failover est en Annexe 9

Conclusion

Au cours de ces dernières années, les réseaux informatiques se sont considérablement étoffés tant par le nombre que par la qualité des services proposés. Les applications sont par ailleurs de plus en plus complexes. Les ressources sont souvent distribuées sur le réseau informatique et les données partagées, plutôt que locales à une station de travail. Le système d'information est situé au cœur de l'entreprise. Aussi, lorsqu'un sinistre se produit, ce sont les fonctions vitales d'une entreprise qui sont touchées (image, productivité, finances). Le faible budget alloué pour le maintenir était insuffisant pour pouvoir adapter l'architecture aux besoins croissants.

Comme bien souvent, c'est seulement une fois que le sinistre s'est produit que l'on a pu en mesurer l'impact. Ce qui a eu pour effet immédiat de débloquer les fonds nécessaires pour ouvrir un projet et rechercher des solutions adaptées. Il est aujourd'hui indispensable d'anticiper en évaluant les risques et en mettant en œuvre un plan de continuité d'activité. C'est donc sans surprise que notre analyse de risques a permis de mettre en évidence les faiblesses du réseau Internet Projet et de l'impact considérable que pouvait entrainer l'exploitation de l'une de ses failles. Le plan d'action immédiatement mis en œuvre consistait en la suppression des SPOF.

Une nouvelle architecture a donc été proposée en s'appuyant sur une infrastructure complètement symétrique illustrée dans un nouveau format du document Visio. Un travail de recherches a été effectué pour déterminer les meilleurs moyens de donner vie à ce dessin. Ces recherches nous ont amenés à choisir une solution adaptée à chaque niveau du réseau (accès, distribution, cœur, accès internet et firewall). Leur mise en œuvre a nécessité d'en maitriser les mécanismes jusqu'au niveau protocolaire. Au-delà la complexité technique, je retiendrai l'importance de la phase préparatoire, de la communication effectuée autour de ce projet, et de la qualité à apporter aux livrables.

Aujourd'hui, la batterie de tests effectués sur le réseau Internet Projet nous permet d'affirmer qu'il est parfaitement redondé[52]. Cette première étape du projet servira de base aux prochaines évolutions, à savoir, la mise en place du mode routé qui aura lieu au cours de l'année prochaine. A ce moment-là, nous nous reposerons les mêmes questions, à

[52] Il reste un équipement sur la chaine ne permet pas de réaliser de redondance à chaud qui est prévu d'être remplacé en 2013.

savoir, quels sont les meilleurs moyens de le mettre en œuvre (HSRP ou VSS). Ce sera également l'occasion de mettre à jour le Plan de Continuité d'Activité et l'ensemble de la documentation associée.

En introduction, nous citions Joël Snyder concernant la fiabilité : « C'est un travail difficile, et cela nécessite de l'intelligence, des compétences et un budget». Nous avons eu le budget !

Bibliographie

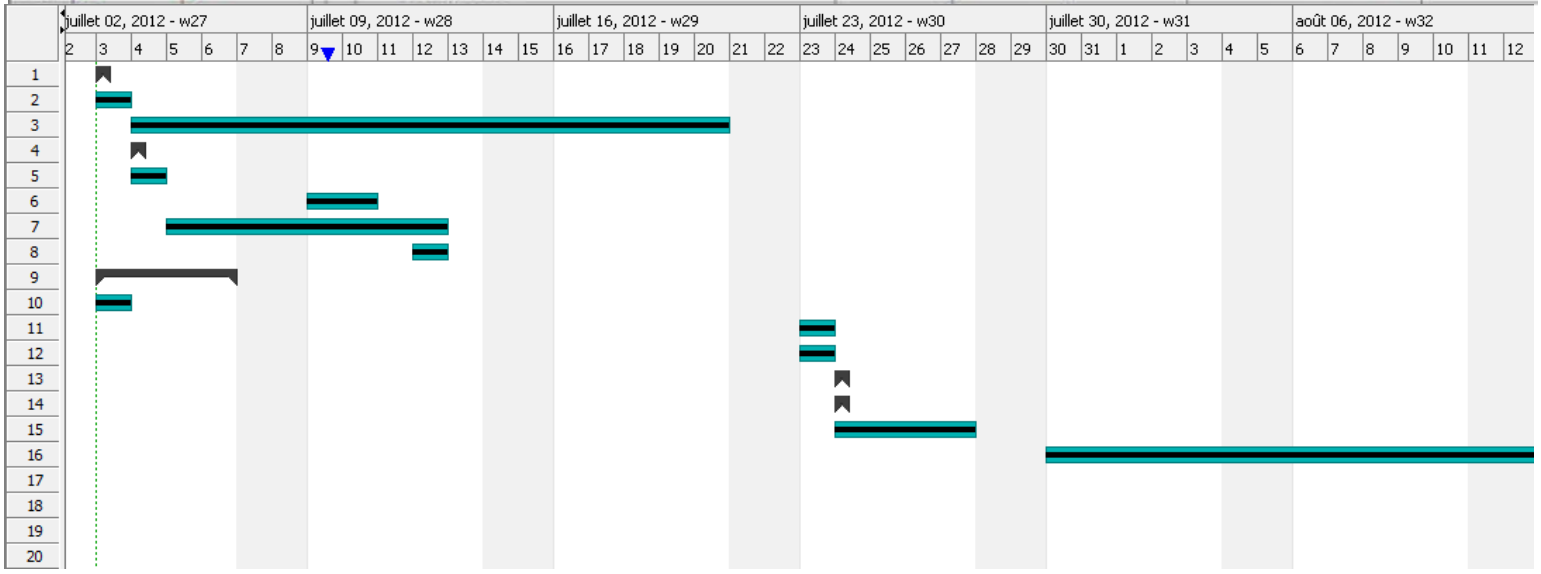
- Astrium – Les activités- [en ligne]. Disponible sur : http://www.astrium.eads.net/fr/our-expertises (consulté le 03/08/2012).
- Bachar Salim HAGGAR – 2010 - Protocoles de Spanning Tree.
- BCI - Management de la continuité d'activité - 2007 (éd. AFNOR).
- Bennasar Matthieu - 2006 - Plan de Continuité d'Activité et Système d'Information : vers l'entreprise résiliente, (Ed. Dunod).
- Cisco - 2007 - Understanding VLAN Trunk Protocol (VTP).
- Cisco - 2007 (Document ID: 11072) - Understanding Issues Related to Inter-VLAN Bridging.
- Clare Gough – 2004 – CCNP BSCI Exam Certification Guide – (Ed Cisco press, Third edition).
- Di Stefano Christophe & Saindzine Wong – 2007 - Les protocoles de redondance HSRP, VRRP et CARP.
- Guidescomparatifs.com – 2008 - Plan de reprise d'activité PRA - PCA Informatique.
- Guinier Daniel – 1995 - Catastrophe et management - Plans d'urgence et continuité des systèmes d'information (Ed. Masson).
- Hucaby David – 2003 – CCNP BCMSN Exam Certification Guide – (Ed Cisco press, Second edition).
- ITIL - 2011 - Méthodologie d'évaluation des Risques [en ligne]. Disponible sur : http://itil.fr/DRP/PCA/methodologie-devaluation-des-risques.html - (consulté le 03/11/2012).
- ITIL - 2011 [en ligne]. Disponible sur : http://itil.fr/ITIL-V2/itil-v2-processus-de-gestion-de-la-continuite-de-service - (consulté le 03/11/2012).
- ITIL - 2011 [en ligne] – Gestion des la disponibilité. Disponible sur : http://itil.fr/ITIL-V2/itil-v2-processus-de-gestion-de-la-disponibilite (consulté le 03/11/2012).

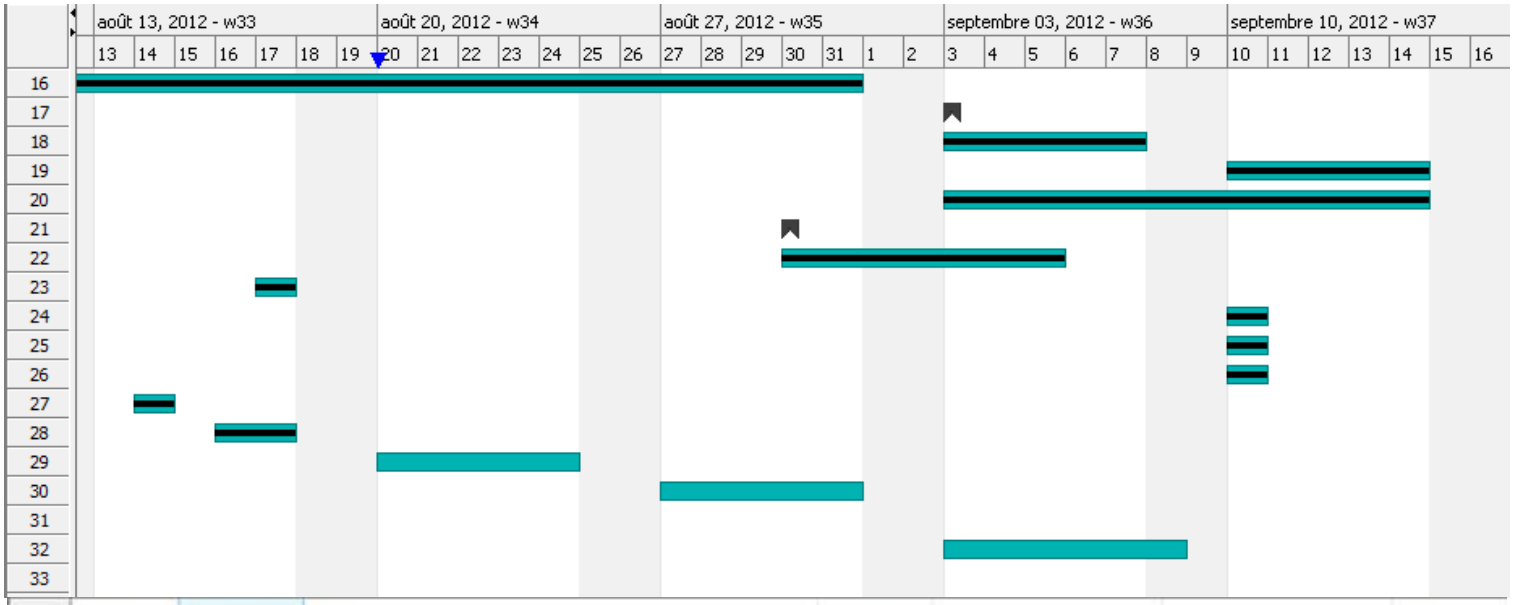
- ITIL - 2011 [en ligne] – Plan de continuité d'activité. Disponible sur : http://itil.fr/DRP/PCA/drppca-mettre-en-oeuvre-un-plan-de-continuite-dactivite (consulté le 03/11/2012).
- Mc Querry Steve – 2002 –Interconnecting Network devices (ICND). Ed. Campus Press, Pearson Education.
- OpenBSD Project – 2012 - Haute disponibilité des pare-feux avec CARP et pfsync. Disponible sur : http://www.openbsd.org - (consulté le 03/11/2012).
- Ryan McBride – 2004 - Firewall Failover with pfsync and CARP.
- télécom-réseaux.net - 2009 - Les mécanismes de redondance de niveau 3 (HSRP, VRRP, GLBP, IRDP) (consulté le 03/11/2012).
- Wald Wojdak - 2003 - CompactPCI and AdvancedTCA Systems.
- Wikipedia – Définitions. Disponibles sur http://en.wikipedia.org/wiki/Main_Page.

Table des annexes

Annexe 1 : Diagramme de Gantt du projet

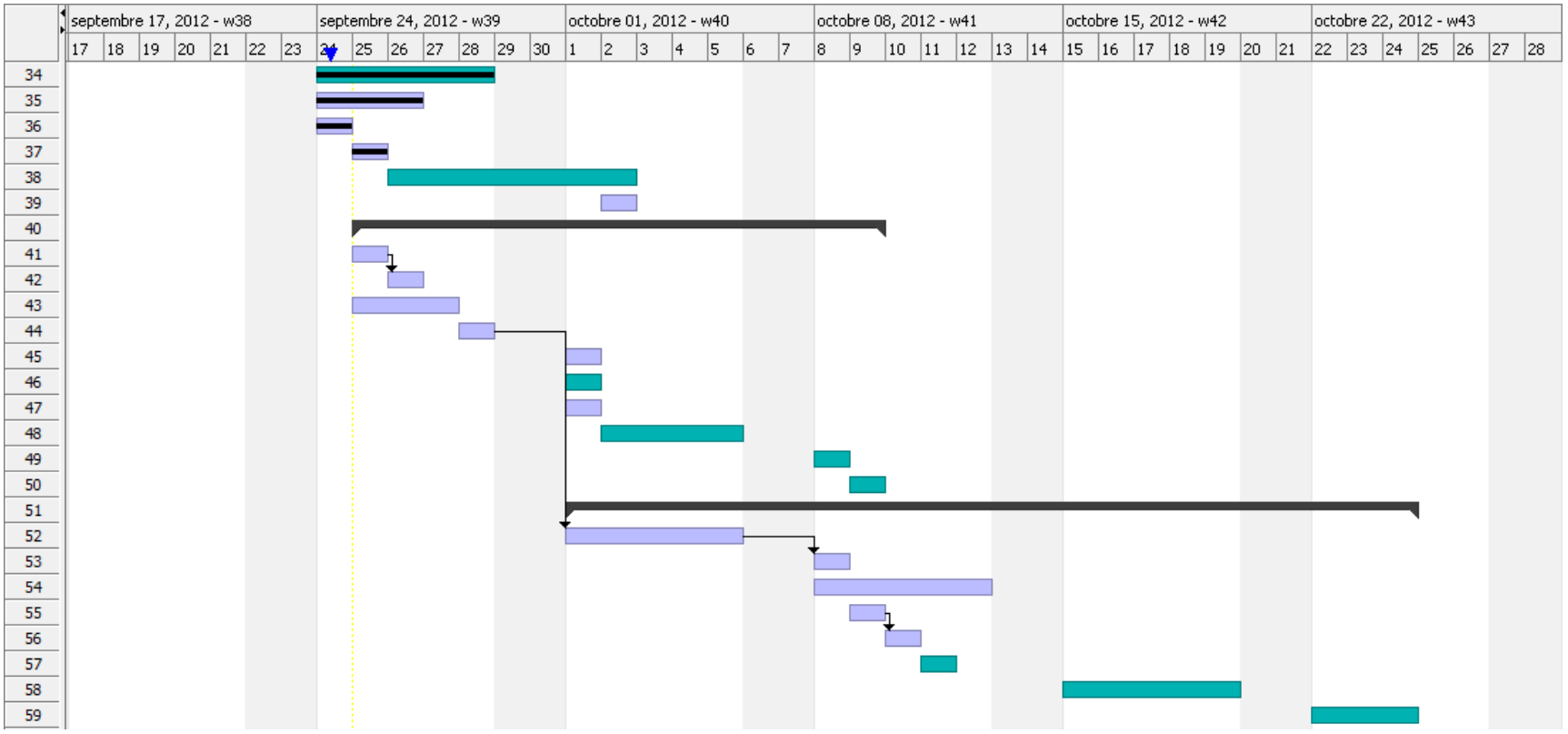
	Indicators	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1			**Mise en place du WiFi**	**0j**	**3 juil. 2012 09:00**	**3 juil. 2012 09:00**	
2			Raccordement des bornes (Suresnes)	1j	3 juil. 2012 09:00	3 juil. 2012 18:00	
3			Raccordement des switches (Suresnes)	13j	4 juil. 2012 09:00	20 juil. 2012 18:00	
4			**Configuration des switches (Suresnes)**	**0j**	**4 juil. 2012 09:00**	**4 juil. 2012 09:00**	
5			tests des 2 derniers switches (Suresnes)	1j	4 juil. 2012 09:00	4 juil. 2012 18:00	
6			recette site (Suresnes)	2j	9 juil. 2012 09:00	10 juil. 2012 18:00	
7			Documentation exploitation	6j	5 juil. 2012 09:00	12 juil. 2012 18:00	
8			Supervision des bornes	1j	12 juil. 2012 09:00	12 juil. 2012 18:00	
9			**Configuration 2ème controlleur**	**4j**	**3 juil. 2012 09:00**	**6 juil. 2012 18:00**	
10			Config @IP admin sur If physique sur CTRL	1j	3 juil. 2012 09:00	3 juil. 2012 18:00	
11			Installation du ctrl en baie bat A (éteint)	1j	23 juil. 2012 09:00	23 juil. 2012 18:00	
12			Mise en place administration outband	1j	23 juil. 2012 09:00	23 juil. 2012 18:00	
13			**Mise à jour du parc**	**0j**	**24 juil. 2012 09:00**	**24 juil. 2012 09:00**	
14			**Mise à jour logicielle**	**0j**	**24 juil. 2012 09:00**	**24 juil. 2012 09:00**	
15			Identification des contacts par projets	4j	24 juil. 2012 09:00	27 juil. 2012 18:00	
16			Mise à jour iOS	25j	30 juil. 2012 09:00	31 août 2012 18:00	





	Indicators	Task Mode	Task Name	Duration	Start	Finish	Predecessors
16	✓		Mise à jour iOS	25j	30 juil. 2012 09:00	31 août 2012 18:00	
17	✓		**Mise à jour matérielle**	**0j**	**3 sept. 2012 09:00**	**3 sept. 2012 09:00**	
18	✓		Vérification emplacement dans les baies	5j	3 sept. 2012 09:00	7 sept. 2012 18:00	
19	✓		Renommage des éqpts sur TLSE (conf, étiquettes, sup)	5j	10 sept. 2012 09:00	14 sept. 2012 18:00	
20	✓		Remplacement des équipements	10j	3 sept. 2012 09:00	14 sept. 2012 18:00	
21			**Administration des équipements**	**0j**	**30 août 2012 09:00**	**30 août 2012 09:00**	
22	✓		Mise en place SSH	5j	30 août 2012 09:00	5 sept. 2012 18:00	
23	✓		Mise en place de comptes nominatifs	1j	17 août 2012 09:00	17 août 2012 18:00	
24	✓		Mise en place cartes additonelles ASAs	1j	10 sept. 2012 09:00	10 sept. 2012 18:00	
25	✓		Routage du SRV S2008 via Tunnel IPSEC	1j	10 sept. 2012 09:00	10 sept. 2012 18:00	
26	✓		Filtrage (RDP only from operationteam to S2008)	1j	10 sept. 2012 09:00	10 sept. 2012 18:00	
27	✓		Administration depuis le serveur S2008	1j	14 août 2012 09:00	14 août 2012 18:00	
28	✓		VPN IPSEC pour administration distante	2j	16 août 2012 09:00	17 août 2012 18:00	
29			Changement du vlan d'administration	5j	20 août 2012 09:00	24 août 2012 18:00	
30			Révision des ACLs sur les switches	5j	27 août 2012 09:00	31 août 2012 18:00	
31			Création de la matrice de flux d'administration	5j	12 nov. 2012 09:00	16 nov. 2012 18:00	
32			Migration de la liaison TAL/IPNG sur ASAs	5,5j	3 sept. 2012 09:00	8 sept. 2012 14:30	

	Indicators	Task Mode	Task Name	Duration	Start	Finish	Predecessors
33			**Gestion des Vlans**	**0j**	**24 sept. 2012 09:00**	**24 sept. 2012 09:00**	
34	✓		Identification des vlans utilisés (ports up) par sw	5j	24 sept. 2012 09:00	28 sept. 2012 18:00	
35	✓		Listing des VLAN non utilisés (passage en VL15)	3j	24 sept. 2012 09:00	26 sept. 2012 18:00	
36	✓		Suppression des VLANs non utilisés.	1j	24 sept. 2012 09:00	24 sept. 2012 18:00	
37	✓		Passage des port VLAN4 vers VLAN 15	1j	25 sept. 2012 09:00	25 sept. 2012 18:00	
38			Migration du serveur VTP	5j	26 sept. 2012 09:00	2 oct. 2012 18:00	
39			Mise à jour des doc, procédures	1j	2 oct. 2012 09:00	2 oct. 2012 18:00	
40			**Installation des équipements**	**11j**	**25 sept. 2012 09:00**	**9 oct. 2012 18:00**	
41			Réserver rocades pour double attachement	1j	25 sept. 2012 09:00	25 sept. 2012 18:00	
42			Préparation/Réservation emplacements dans les baies	1j	26 sept. 2012 09:00	26 sept. 2012 18:00	41
43			Préparation des fibres pour bat vers 4500	3j	25 sept. 2012 09:00	27 sept. 2012 18:00	
44			Installation du 4500 Bat R	1j	28 sept. 2012 09:00	28 sept. 2012 18:00	
45			Installation efficient IP (éteints)	1j	1 oct. 2012 09:00	1 oct. 2012 18:00	
46			Installation du 2ème ASA bat A (éteint)	1j	1 oct. 2012 09:00	1 oct. 2012 18:00	
47			Installation du TLS2960-A0LT2-PROJINT (éteint)	1j	1 oct. 2012 09:00	1 oct. 2012 18:00	
48			Installation du 2ème BlueSocket Bat A (éteint)	4j	2 oct. 2012 09:00	5 oct. 2012 18:00	
49			Installation du 4500 Bat A (éteint)	1j	8 oct. 2012 09:00	8 oct. 2012 18:00	
50			Installation efficient IP Bat A (éteint)	1j	9 oct. 2012 09:00	9 oct. 2012 18:00	
51			**Migration sur le cœur de réseau Bat R**	**18j**	**1 oct. 2012 09:00**	**24 oct. 2012 18:00**	
52			Migration des 3750 vers 4500 bat R	5j	1 oct. 2012 09:00	5 oct. 2012 18:00	44
53			MàJ description des ports sur le 4500	1j	8 oct. 2012 09:00	8 oct. 2012 18:00	52
54			Mise à jour doc (schéma)	5j	8 oct. 2012 09:00	12 oct. 2012 18:00	
55			Migration du BlueSocket du 3560 vers le 4500	1j	9 oct. 2012 09:00	9 oct. 2012 18:00	
56			Migration du 3560 du 3750 vers le 4500	1j	10 oct. 2012 09:00	10 oct. 2012 18:00	55
57			Installation du TLS2960-A0LT1-PROJINT (frontal)	1j	11 oct. 2012 09:00	11 oct. 2012 18:00	
58			Migration du serveur VTP du 3560 vers le 4500	5j	15 oct. 2012 09:00	19 oct. 2012 18:00	
59			Migration de la Fibre noire (SPOT, Astrolabe)	3j	22 oct. 2012 09:00	24 oct. 2012 18:00	


septembre 17, 2012 - w38
septembre 24, 2012 - w39
octobre 01, 2012 - w40
octobre 08, 2012 - w41
octobre 15, 2012 - w42
octobre 22, 2012 - w43
17 18 19 20 21 22 23 24 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59

Annexe 2 : Plan de continuité d'activité détaillé

Extrait d'ITIL : http://itil.fr/DRP/PCA/drppca-mettre-en-oeuvre-un-plan-de-continuite-dactivite

I.1.1.1 PLAN DE SAUVEGARDE

Le plan de sauvegarde se situe en amont du sinistre, c'est la phase préparatoire lors de laquelle on va non seulement identifier les scénarii de sinistralité, mais aussi construire la réponse à ce sinistre.

Avant d'aller plus loin dans le projet vous devez prévoir le mode de continuité choisi :

- Continuité de service intégrale sans coupure,
- Continuité de service intégrale avec coupure,
- Continuité de service partielle avec/sans coupure (mode dégradé).

Les décisions prises à ce stade vont définir les dispositions mises en œuvre dans votre plan de secours. Il est donc important de ramener ce choix à la cartographie des risques réalisées au préalable et rapportée aux enjeux business pour votre organisation. À titre d'exemple, pour une organisation qui ne facturerait pas ses clients en internes, la comptabilité interne n'est pas un service critique. Aussi le management pourra décider de ne pas l'inclure dans l'option de reprise "continuité partielle".

I.1.1.1.1 PLAN DE SECOURS

L'objectif du plan de secours est de réduire ou limiter l'impact d'un sinistre. L'étape de construction est donc la clé de voute des opérations qui seront réalisées à terme.

Le plan de secours doit :

- être aligné sur risques vitaux de l'entreprise,
- intégrer les enjeux business de l'organisation,
- ajuster les dispositions de secours à ces enjeux,

- être aligné avec la grille des risques,
- être évaluable sur la base d critères tangibles (eg : nombre de service redémarrés en moins de 8 heures),
- inclure la durée d'indisponibilité tolérée,
- inclure la liste des services redémarrés après coupure,
- inclure la liste des services sans interruption,
- intégrer les mesures curatives,
- intégrer les contre-mesures mis déployées pour réduire les risques majeurs

I.1.1.1.2 DISPOSITIONS TECHNIQUES ET ARCHITECTURALE

Le plan de secours peut être scindé en 3 sections.

Les dispositions techniques et architecturales couvrent l'ensemble des moyens techniques à mettre à déployer en amont.

Selon la typologie du plan de continuité adressé son périmètre couvrira :

- Les salles aussi bien les biens d'équipements,
- Les données disponibles et intègres sur les systèmes,
- Les applications et systèmes pré installés et pré configurés sur l'environnement de secours,
- Des réseaux de données disponibles,
- Des réseaux téléphoniques disponibles,
- Une architecture de sauvegarde sur le site distant.

Une fois les choix actés, il faut les faire valider par le management.

I.1.1.1.3 DISPOSITIONS PROCEDURALES

Si le dispositif technique constitue le socle du PCA, l'enjeu du projet porte véritablement sur l'organisation et notamment sur sa capacité à fonctionner dans un contexte de sinistre. En effet, après que le sinistre soit intervenu il est possible que les locaux, les équipements, le téléphone ne soient plus accessibles.

C'est pourquoi les dispositions procédurales et documentaires vont permettre à l'organisation de préparer, puis de formaliser les dispositions opérationnelles à réaliser une fois la survenance du sinistre.

Les procédures et processus doivent être formalisés, diffusés, compris et maitrisés.

- ***Documentation***

La documentation doit rassembler tous les éléments nécessaires à l'exécution du PCA, il s'agit :

- des procédures de restauration et de sauvegarde,
- des documents fonctionnels tels que la remise en service des applications métiers,
- des documents décrivant les membres de la cellule de crise,
- liste des numéros des numéros de téléphones des spécialistes, des fournisseurs, des mainteneurs, éditeurs, etc.

Les documents doivent être accessibles en format électronique et papier sur site. Bien entendu seules les dernières versions autorisées doivent être mises à disposition.

- ***Procédures d'intervention***

Les procédures d'intervention décrivent le mode de bascule opérationnel. Elles doivent inclure :

- Les rôles et responsabilité,
- Les modes opératoires,
- Les formulaires type de document,
- Les instructions de travail,
- Les procédures de soutient, de communication, durant la crise.

I.1.1.1.4 DISPOSITIONS ORGANISATIONNELLES

Les dispositions organisationnelles prévoient l'organisation qui sera mise en branle durant la crise. Elles doivent être exhaustives et bâties au regard de la législation, notamment par rapport au code du travail.

N'oubliez pas d'intégrer les dispositions purement "logistique" telles que la mise à disposition de locaux, bureaux, téléphones, ordinateur, connexions réseaux, etc.

- ***Habilitation***

Les personnes habilitées doivent être identifiées en amont de la crise, cela tombe sous le sens. Car dans l'hypothèse d'un sinistre certaines personnes devront non seulement avoir accès aux locaux distants, au téléphone, mais aussi accès aux librairies de sauvegarde, aux applications, aux accès d'administration pour reconfigurer un logiciel, etc.

- ***Formation***

Durant toutes les phases de mise en place du PCA il est indispensable de vous assurez que les équipes comprennent l'importance de leur rôle dans l'exécution du plan. À ce titre il est nécessaire d'une part de sensibiliser sur les enjeux du Plan de Continuité, et d'autre part de former les équipes qui assureront la reprise.

- ***Cellule de crise***

La cellule de crise est constituée en amont de l'occurrence du sinistre. Veillez à la maintenir à jour au grès du turn-over par exemple.

La cellule doit être constituée de manager, y compris de la direction, de la direction technique, logistique, etc. Selon les risques et services identifiés comme prioritaire lors de l'analyse des risques.

La cellule de crise doit inclure des dispositions concernant la communication vers l'extérieur, afin d'assurer un relai vers les parties prenantes, clients, actionnaires, presses, etc.

Une liste nominative doit être dressée et communiquée, et doit contenir les numéros de téléphone, email, etc. à contacter en cas de crise.

- ***Contrats de travail***

L'hypothèse de la survenance d'un sinistre peut vous amener à modifier momentanément la durée légale de travail de vos collaborateurs. Il faut donc vous prémunir juridiquement de cet écart en précisant par exemple dans vos contrats que les collaborateurs pourraient être amen, le cas échéant, à travailler davantage de onze heures d'affiliées.

La cellule de crise doit être suffisamment "staffée" pour permettre l'exécution du plan de reprise, et de retour à une situation nominale.

I.1.1.2 PLAN DE REPRISE

C'est l'exécution du dispositif lors de l'occurrence du sinistre. Le plan de reprise permet de relancer l'activité selon des modalités définies lors de la constitution du plan de sauvegarde. Il se situe dans le contexte du sinistre.

I.1.1.3 PLAN DE RETOUR A LA NORMALE

Le plan de retour à la normale dresse la liste des opérations à réaliser pour revenir à la situation antérieure au sinistre. Selon les services qui ont été visés par le plan de reprise, il s'agira de remettre tous les services en lignes et accessibles.

I.1.1.4 PLAN DE TESTS

Le principal facteur de succès du plan de continuité est le test. Le plan de test a pour objectif de valider que l'organisation, les procédures, les documents, etc. seront correctement ajustés pour que le plan soit une réussite. À cet effet le plan de test doit être réalisé régulièrement et dans des conditions proches de la "vraie vie.

Les changements organisationnels, techniques, etc. doivent être répercutés sur le plan afin d'en garantir l'exactitude.

I.1.1.4.1 TEST THEORIQUE

Le test théorique est la première étape. Lorsque vous avez formalisé les dispositions du plan de reprise, il vous faut les tester, afin de vérifier si les étapes s'enchainent chronologiquement, si les procédures sont efficaces, si les documents sont complets, si les équipes sont formées, si les applications et serveurs sont prêts, etc.

Le test théorique est un test "papier" dans le sens ou il n'impacte pas les opérations et ne nécessite pas d'interruption de Services.

I.1.1.4.2 PRE-TESTS ET TESTS PARTIELS

Le pré-test est quant à lui un vrai test. Il peut soit concerner une partie des services éligibles dans votre plan de secours, soit une partie des dispositions de secours telle que la reprise de données par exemple.

Une approche judicieuse, en amont de plan complet, et de tester chacune des dispositions et de relever les dysfonctionnements le cas échéant. Ainsi vous pourrez ajuster les dispositions techniques et organisationnelles avant le test final.

I.1.1.4.3 TEST COMPLET

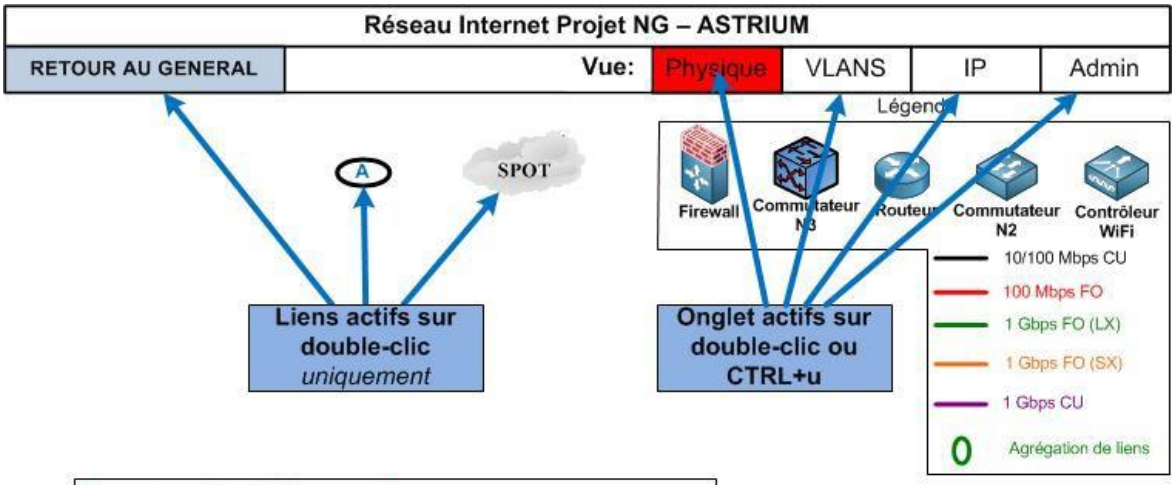
Le test dit "complet" est comme son nom l'indique complet. C'est à dire qu'il a pour but de valider que le plan de continuité sera réalisé dans les conditions réels de sinistre. S'il est difficile de le mettre véritablement en œuvre c'est toutefois la seule garantie que vous aurez quant à son adéquation le jour "j".

I.1.1.5 PLAN DE MAINTENANCE

Dès lors que vous avez réalisés toutes ces étapes, le travail n'est hélas pas terminé. En effet les organisations sont en perpétuelles évolutions. Nouveaux services/produits, nouvelles organisations, nouvelles équipes, nouveaux logiciels, nouveaux sites, etc.

Autant de paramètres qu'il va falloir surveiller de près et surtout intégrer au dispositif de continuité d'activité. À ce titre vous devrez probablement réaliser une nouvelle itération de l'analyse des risques, puis des modifications du PCA, et enfin pratiquer de nouveaux tests.

Annexe 3 : Schémas d'Internet Projet



Composants du document

6 calques :
- **Fond** : Trame de fond, bâtiments et locaux techniques
- **Equipements** : Equipements réseaux et serveurs
- **Physique** : Informations de niveau 1 (ports, câblage)
- **VLAN** : Informations de niveau 2 (VLAN, STP)
- **IP** : Adressage IP
- **Admin** : Adresses IP d'administration

4 onglets : (basés sur différents calques):
- **Physique** : Fond + Equipements + Physique
- **VLAN** : Fond + Equipements + VLAN
- **IP** : Fond + Equipements + IP
- **Admin** : Fond + Equipements + Admin

Modification du document:
Afin de conserver l'utilité du document, il est important d'observer quelques règles d'usage:
- Préférer les copier/coller (afin de conserver l'affectation au bon calque),
- Affecter l'objet au bon calque,
- Vérifier la superposition des calques avant d'enregistrer.

Sauvegarde du document:
Afin de conserver les fonctionnalités du document, il est important d'observer quelques règles d'usage:
- Conserver le nom du fichier (« Internet Projet NG ») et des onglets,
- Ne pas déplacer le fichier (afin de conserver les liens hypertextes),
- Enregistrer la version courante du document dans le dossier « archive » en incrémentant le numéro de version dans le nom (« Internet Projet NG v1.1»),
- Réaliser le versionning dans le cartouche du Schéma Général.

Figure 23: Fonctionnement du document Visio

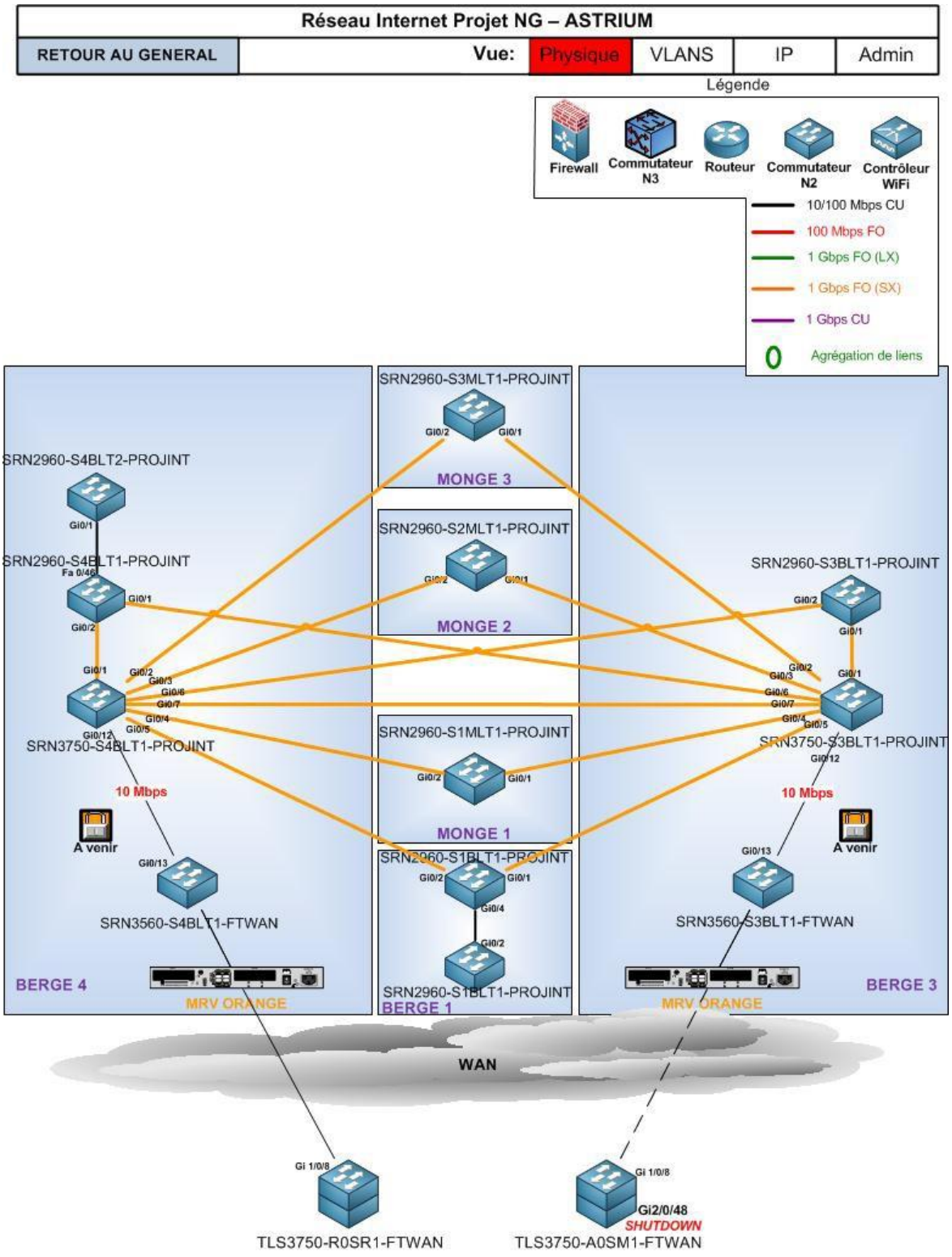


Figure 24 : Calque représentant une vue physique d'un site distant

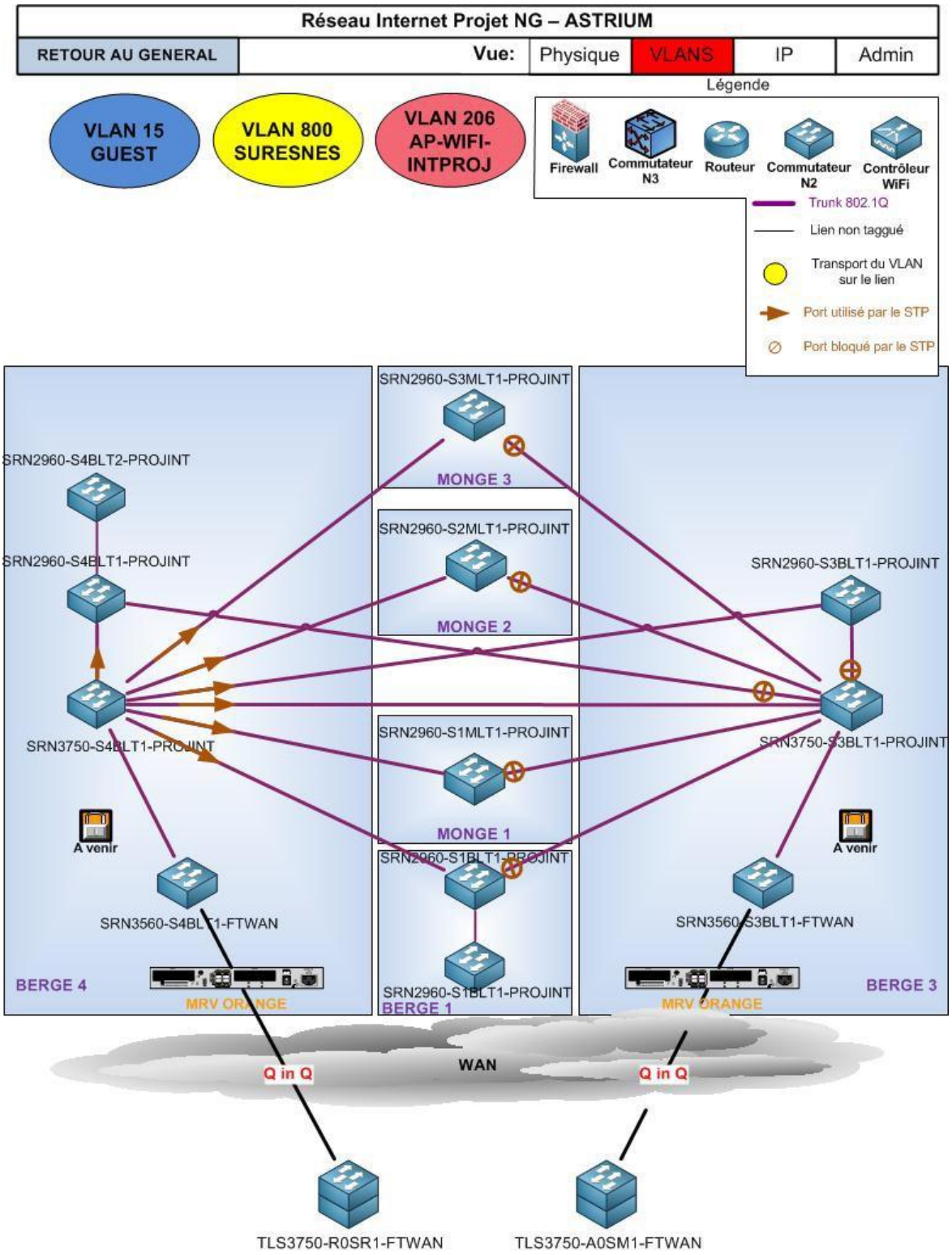


Figure 25 : Calque représentant le niveau 2 (Vlan et STP) d'un site distant

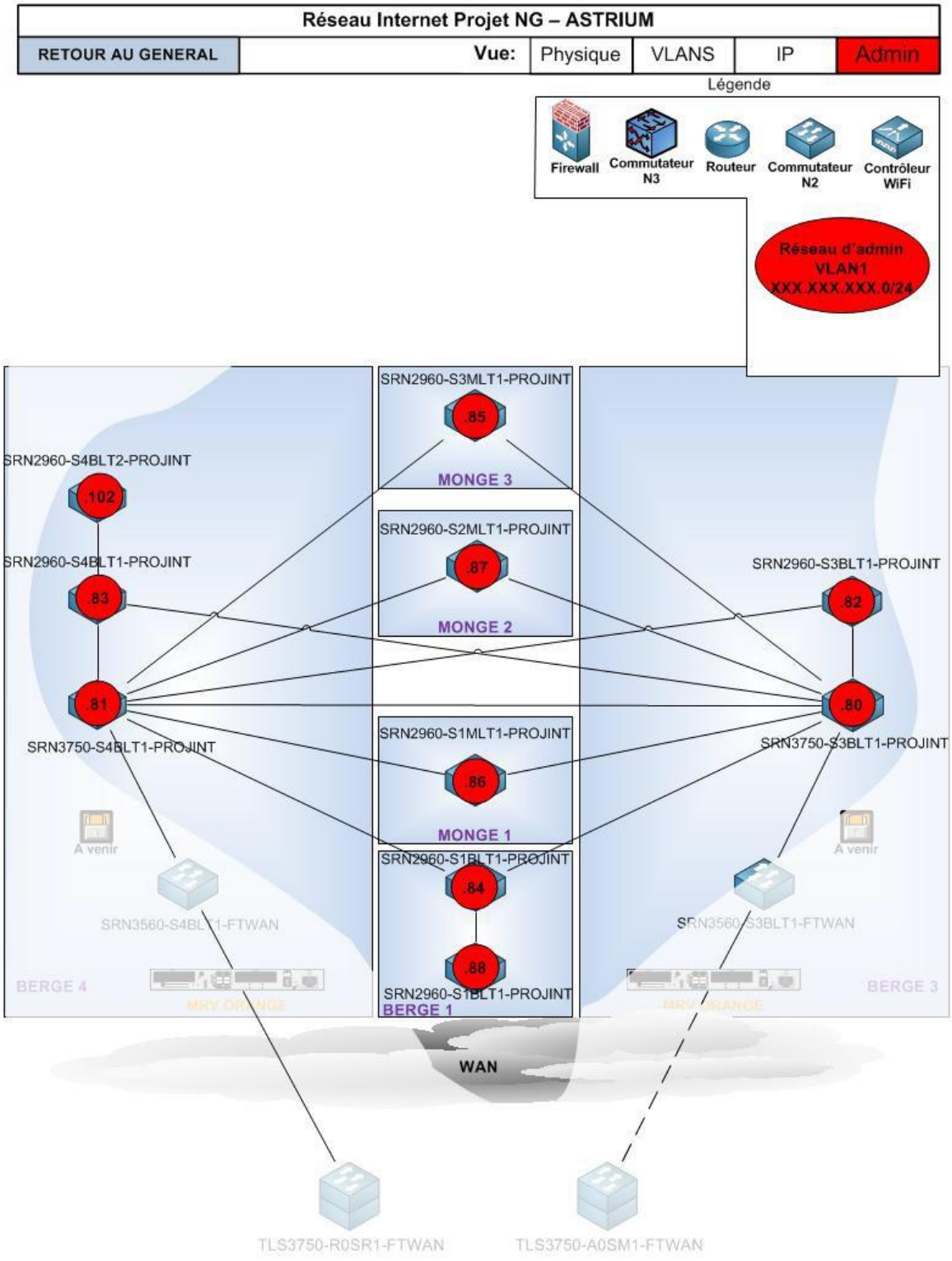


Figure 26 : Calque représentant les adresses d'administration

Annexe 4 : Macro de changement de calque

```
      Attribute VB_Name = "NewMacros"

      Sub Changer_calque()
      Attribute Changer_calque.VB_ProcData.VB_Invoke_Func = "u"
'
' Tout objet du document Visio est associé à un calque (on peut afficher
cette propriété en faisant un clic-droit
' sur l'objet -> Format -> Calque).
' En associant les objets aux calques adéquats (ex:@IP dans le calque IP,
n° de VLAN dans la calque VLAN),
' on peut utiliser la propriété visLayerVisible du calque pour afficher
tous les objets d'un coup
'
'Pour afficher l'ID d'un objet: clic-droit sur l'objet -> Format ->
Special
'
' Raccourci clavier : Ctrl+u
'
'On définit une variable pour chaque calque
            Dim UndoScopeID1 As Long
            Dim vsoLayer1 As Visio.Layer

'Les variables suivantes vont nous permettre de compter le nombre de
calques existnts sur la page active
'Pour ensuite pouvoir retrouver parmi eux les 7 calques qu'on utilise
'Pour cela,il faut juste que les calques aient les noms corrects!!!!
            Dim nbCalques, i As Integer

'Variable qui sera affectée au calque contenant les informations
relatives aux VLANs et au STP
            Dim VLAN As Visio.Layer

'Variable qui sera affectée au calque contenant les informations de
raccordement Physique
            Dim Physique As Visio.Layer

'Variable qui sera affectée au calque contenant l'ensemble des
équipements réseaux
            Dim Equipements As Visio.Layer

'Variable qui sera affectée au calque contenant la localisation des
équipements
            Dim Fond As Visio.Layer

'Variable qui sera affectée au calque contenant les informations
nécessaires à l'administration des équipements réseaux
            Dim Admin As Visio.Layer

'On associe chaque calque à la variable correspondante (variables
globales)
'l'ID de chaque calque correspond à l'ordre visible dans Format -> Calque
            UndoScopeID1 = Application.BeginUndoScope("Propriétés des
calques")

'Cette variable est utilisée temporairement dans le Select-Case pour
récupérer les noms des calques
```

```
Dim Calque As Visio.Layer


'On compte le nombre de calques de la page active
            nbCalques = Application.ActivePage.Layers.Count()

'Pour chacun des calques de la page, on va récupérer son nom, ce qui va
nous permettre d'affecter le calque à la variable correspondante
            For i = 1 To nbCalques
            Set Calque = Application.ActiveWindow.Page.Layers.Item(i)
            Select Case Calque.Name()
                  Case "VLAN"
                        Set VLAN = Calque
                  Case "Fond"
                        Set Fond = Calque
                  Case "Physique"
                        Set Physique = Calque
                  Case "Equipements"
                        Set Equipements = Calque
                  Case "IP"
                        Set IP = Calque
                  Case "Admin"
                        Set Admin = Calque
            End Select
            Next

'Par défaut, on affiche les calques Fond, et Equipements
'Equipements est affiché dans tous les cas sauf pour la vue IP pour des
raisons de lisibilité
'Puis, selon le choix de l'utilisateur, on affichera sélectivement les
autres calques
            Fond.CellsC(visLayerVisible).FormulaU = "1"
            Fond.CellsC(visLayerPrint).FormulaU = "1"
            Equipements.CellsC(visLayerVisible).FormulaU = "1"
            Equipements.CellsC(visLayerPrint).FormulaU = "1"


'Les calques sont classés arbitrairement (parce qu'on trouve ça logique!)
dans l'ordre suivant:
' Physique -> VLAN -> IP -> Admin
'Parmi les 4 calques restants, on identifie le calque visible puis on
masque tous ces calques sauf le calque suivant

            If Physique.CellsC(visLayerVisible).FormulaU Then
                  Physique.CellsC(visLayerVisible).FormulaU = "0"
                  Physique.CellsC(visLayerPrint).FormulaU = "0"
                  VLAN.CellsC(visLayerVisible).FormulaU = "1"
                  VLAN.CellsC(visLayerPrint).FormulaU = "1"
                  IP.CellsC(visLayerVisible).FormulaU = "0"
                  IP.CellsC(visLayerPrint).FormulaU = "0"
                  Admin.CellsC(visLayerVisible).FormulaU = "0"
                  Admin.CellsC(visLayerPrint).FormulaU = "0"

            ElseIf VLAN.CellsC(visLayerVisible).FormulaU Then
                  Physique.CellsC(visLayerVisible).FormulaU = "0"
                  Physique.CellsC(visLayerPrint).FormulaU = "0"
                  VLAN.CellsC(visLayerVisible).FormulaU = "0"
                  VLAN.CellsC(visLayerPrint).FormulaU = "0"
                  IP.CellsC(visLayerVisible).FormulaU = "1"
                  IP.CellsC(visLayerPrint).FormulaU = "1"
                  Admin.CellsC(visLayerVisible).FormulaU = "0"
```

```
Admin.CellsC(visLayerPrint).FormulaU = "0"


            ElseIf IP.CellsC(visLayerVisible).FormulaU Then
                  Physique.CellsC(visLayerVisible).FormulaU = "0"
                  Physique.CellsC(visLayerPrint).FormulaU = "0"
                  VLAN.CellsC(visLayerVisible).FormulaU = "0"
                  VLAN.CellsC(visLayerPrint).FormulaU = "0"
                  IP.CellsC(visLayerVisible).FormulaU = "0"
                  IP.CellsC(visLayerPrint).FormulaU = "0"
                  Admin.CellsC(visLayerVisible).FormulaU = "1"
                  Admin.CellsC(visLayerPrint).FormulaU = "1"


            Else
                  Physique.CellsC(visLayerVisible).FormulaU = "1"
                  Physique.CellsC(visLayerPrint).FormulaU = "1"
                  VLAN.CellsC(visLayerVisible).FormulaU = "0"
                  VLAN.CellsC(visLayerPrint).FormulaU = "0"
                  IP.CellsC(visLayerVisible).FormulaU = "0"
                  IP.CellsC(visLayerPrint).FormulaU = "0"
                  Admin.CellsC(visLayerVisible).FormulaU = "0"
                  Admin.CellsC(visLayerPrint).FormulaU = "0"


            End If
            Application.EndUndoScope UndoScopeID1, True

      End Sub


      Sub Changer_calquePhysique()

            Dim UndoScopeID1 As Long
            Dim vsoLayer1 As Visio.Layer
            Dim IP As Visio.Layer
            Dim VLAN As Visio.Layer
            Dim Physique As Visio.Layer
            Dim Equipements As Visio.Layer
            Dim Fond As Visio.Layer
            Dim Admin As Visio.Layer

            UndoScopeID1 = Application.BeginUndoScope("Propriétés des
calques"
)

'Cette variable est utilisée temporairement dans le Select-Case pour
récupérer les noms des calques
            Dim Calque As Visio.Layer


'On compte le nombre de calques de la page active
            nbCalques = Application.ActivePage.Layers.Count()

'Pour chacun des calques de la page, on va récupérer son nom, ce qui va
nous permettre d'affecter le calque à la variable correspondante
            For i = 1 To nbCalques
            Set Calque = Application.ActiveWindow.Page.Layers.Item(i)
            Select Case Calque.Name()
                  Case "VLAN"
                        Set VLAN = Calque
                  Case "Fond"
```

```
Set Fond = Calque
                  Case "Physique"
                        Set Physique = Calque
                  Case "Equipements"
                        Set Equipements = Calque
                  Case "IP"
                        Set IP = Calque
                  Case "Admin"
                        Set Admin = Calque
            End Select
            Next

'Par défaut, on affiche les calques Fond, et Equipements
'Equipements est affiché dans tous les cas sauf pour la vue IP pour des
raisons de lisibilité
'Parmi les 4 calques restants, on affiche le calque Physique et on masque
les autres
            Physique.CellsC(visLayerVisible).FormulaU = "1"
            Physique.CellsC(visLayerPrint).FormulaU = "1"
            VLAN.CellsC(visLayerVisible).FormulaU = "0"
            VLAN.CellsC(visLayerPrint).FormulaU = "0"
            IP.CellsC(visLayerVisible).FormulaU = "0"
            IP.CellsC(visLayerPrint).FormulaU = "0"
            Admin.CellsC(visLayerVisible).FormulaU = "0"
            Admin.CellsC(visLayerPrint).FormulaU = "0"

            Application.EndUndoScope UndoScopeID1, True

      End Sub

      Sub Changer_calqueVLAN()

            Dim UndoScopeID1 As Long
            Dim vsoLayer1 As Visio.Layer
            Dim IP As Visio.Layer
            Dim VLAN As Visio.Layer
            Dim Physique As Visio.Layer
            Dim Equipements As Visio.Layer
            Dim Fond As Visio.Layer
            Dim Admin As Visio.Layer

            UndoScopeID1 = Application.BeginUndoScope("Propriétés des
calques")


'Cette variable est utilisée temporairement dans le Select-Case pour
récupérer les noms des calques
             Dim Calque As Visio.Layer

'On compte le nombre de calques de la page active
            nbCalques = Application.ActivePage.Layers.Count()

'Pour chacun des calques de la page, on va récupérer son nom, ce qui va
nous permettre d'affecter le calque à la variable correspondante
            For i = 1 To nbCalques
            Set Calque = Application.ActiveWindow.Page.Layers.Item(i)
            Select Case Calque.Name()
                  Case "VLAN"
                        Set VLAN = Calque
                  Case "Fond"
                        Set Fond = Calque
```

```
Case "Physique"
                        Set Physique = Calque
                  Case "Equipements"
                        Set Equipements = Calque
                  Case "IP"
                        Set IP = Calque
                  Case "Admin"
                        Set Admin = Calque
            End Select
            Next



'Par défaut, on affiche les calques Fond, et Equipements
'Equipements est affiché dans tous les cas sauf pour la vue IP pour des
raisons de lisibilité
'Parmi les 4 calques restants, on affiche le calque Physique et on masque
les autres
            Physique.CellsC(visLayerVisible).FormulaU = "0"
            Physique.CellsC(visLayerPrint).FormulaU = "0"
            VLAN.CellsC(visLayerVisible).FormulaU = "1"
            VLAN.CellsC(visLayerPrint).FormulaU = "1"
            IP.CellsC(visLayerVisible).FormulaU = "0"
            IP.CellsC(visLayerPrint).FormulaU = "0"
            Admin.CellsC(visLayerVisible).FormulaU = "0"
            Admin.CellsC(visLayerPrint).FormulaU = "0"

            Application.EndUndoScope UndoScopeID1, True

      End Sub


      Sub Changer_calqueAdmin()

            Dim UndoScopeID1 As Long
            Dim vsoLayer1 As Visio.Layer
            Dim IP As Visio.Layer
            Dim VLAN As Visio.Layer
            Dim Physique As Visio.Layer
            Dim Equipements As Visio.Layer
            Dim Fond As Visio.Layer
            Dim Admin As Visio.Layer

            UndoScopeID1 = Application.BeginUndoScope("Propriétés des
calques"
)


'Cette variable est utilisée temporairement dans le Select-Case pour
récupérer les noms des calques
            Dim Calque As Visio.Layer


'On compte le nombre de calques de la page active
            nbCalques = Application.ActivePage.Layers.Count()

'Pour chacun des calques de la page, on va récupérer son nom, ce qui va
nous permettre d'affecter le calque à la variable correspondante
            For i = 1 To nbCalques
            Set Calque = Application.ActiveWindow.Page.Layers.Item(i)
            Select Case Calque.Name()
                  Case "VLAN"
```

```
Set VLAN = Calque
                  Case "Fond"
                        Set Fond = Calque
                  Case "Physique"
                        Set Physique = Calque
                  Case "Equipements"
                        Set Equipements = Calque
                  Case "IP"
                        Set IP = Calque
                  Case "Admin"
                        Set Admin = Calque
            End Select
            Next

'Par défaut, on affiche les calques Fond, et Equipements
'Equipements est affiché dans tous les cas sauf pour la vue IP pour des
raisons de lisibilité
'Parmi les 4 calques restants, on affiche le calque Physique et on masque
les autres
            Physique.CellsC(visLayerVisible).FormulaU = "0"
            Physique.CellsC(visLayerPrint).FormulaU = "0"
            VLAN.CellsC(visLayerVisible).FormulaU = "0"
            VLAN.CellsC(visLayerPrint).FormulaU = "0"
            IP.CellsC(visLayerVisible).FormulaU = "0"
            IP.CellsC(visLayerPrint).FormulaU = "0"
            Admin.CellsC(visLayerVisible).FormulaU = "1"
            Admin.CellsC(visLayerPrint).FormulaU = "1"

            Application.EndUndoScope UndoScopeID1, True

      End Sub

      Sub Changer_calqueIP()

            Dim UndoScopeID1 As Long
            Dim vsoLayer1 As Visio.Layer
            Dim IP As Visio.Layer
            Dim VLAN As Visio.Layer
            Dim Physique As Visio.Layer
            Dim Equipements As Visio.Layer
            Dim Fond As Visio.Layer
            Dim Admin As Visio.Layer

            UndoScopeID1 = Application.BeginUndoScope("Propriétés des
calques"
)


'Cette variable est utilisée temporairement dans le Select-Case pour
récupérer les noms des calques
            Dim Calque As Visio.Layer

'On compte le nombre de calques de la page active
            nbCalques = Application.ActivePage.Layers.Count()

'Pour chacun des calques de la page, on va récupérer son nom, ce qui va
nous permettre d'affecter le calque à la variable correspondante
            For i = 1 To nbCalques
            Set Calque = Application.ActiveWindow.Page.Layers.Item(i)
            Select Case Calque.Name()
                  Case "VLAN"
                        Set VLAN = Calque
```

```
Case "Fond"
                        Set Fond = Calque
                  Case "Physique"
                        Set Physique = Calque
                  Case "Equipements"
                        Set Equipements = Calque
                  Case "IP"
                        Set IP = Calque
                  Case "Admin"
                        Set Admin = Calque
            End Select
            Next


'Par défaut, on affiche les calques Fond, et Equipements
'Equipements est affiché dans tous les cas sauf pour la vue IP pour des
raisons de lisibilité
'Parmi les 4 calques restants, on affiche le calque Physique et on masque
les autres
            Physique.CellsC(visLayerVisible).FormulaU = "0"
            Physique.CellsC(visLayerPrint).FormulaU = "0"
            VLAN.CellsC(visLayerVisible).FormulaU = "0"
            VLAN.CellsC(visLayerPrint).FormulaU = "0"
            IP.CellsC(visLayerVisible).FormulaU = "1"
            IP.CellsC(visLayerPrint).FormulaU = "1"
            Admin.CellsC(visLayerVisible).FormulaU = "0"
            Admin.CellsC(visLayerPrint).FormulaU = "0"

            Application.EndUndoScope UndoScopeID1, True

      End Sub
```

Annexe 5 : Principe du QinQ

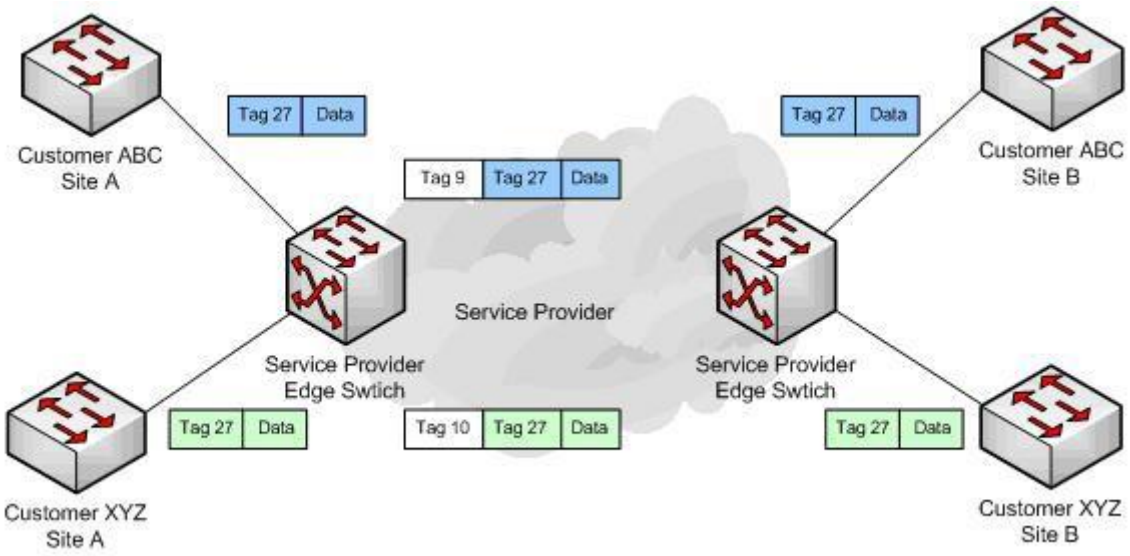


Figure 27 : Schéma de principe du QinQ[53]

La norme 802.1q, permettant l'utilisation de VLANs, ajoute 4 octets dans l'en-tête de la trame Ethernet (on parle de trame Ethernet « taggé » ou VLAN « taggé »), répartis dans 2 champs distincts :

- Le champ TPI (*Tag Protocol Identifier*) ou *Ethertype* sur 2 octets, pour l'identification du type de trame Ethernet : sa valeur en hexadécimal est 0x8100

- le champ TCI (*Tag Control Information*) sur 2 octets, pour l'identification du VLAN

(*VLAN Identifier* qui correspond au numéro de tag) et une éventuelle priorité si une politique de QoS existe (norme 802.1p). Le nombre de VLANs est limité à 4 096.

Pour augmenter le nombre de VLANs possibles ou par exemple faciliter la propagation de plusieurs VLANs inter-site (*Customer*, C-VLAN) sur un opérateur dans un seul et même « super VLAN » (*Service*, S-VLAN), l'IEEE a défini une nouvelle norme : 802.1ad, connue sous le nom de *Provider Bridge Network*, aussi désignée sous le sigle « Q-in-Q ».

On regroupe plusieurs VLANs dans un « super VLAN » en ajoutant 4 octets dans l'en-tête de la trame Ethernet taggée, devant les champs TPI/TCI indiquant le tag du VLAN de site

[53] Source : http://irwanp.wordpress.com/2008/06/23/qinq-8021q-tunneling-on-cisco-switches/

(que l'on peut maintenant nommer C-TPI et C-TCI, avec C pour *Customer*), deux nouveaux champs :

- Le champ S-TPI (*Service Tag Protocol Identifier*) sur 2 octets, pour l'identification du type de trame Ethernet :

o L'IEEE recommande l'utilisation de la valeur 0x88a8

o Mais il est fréquent que la valeur d'identification 0x8100 d'une trame Ethernet taggée soit réutilisée (la trame comporte alors 2 fois cette valeur C-TPI et STPI).

- Le champ S-TCI (*Service Tag Control Information*) pour l'identification du « Super VLAN » avec un numéro de tag.

La trame est ainsi « double-taggée ». Elle comporte un *outer tag* aussi appelé « VMAN tag» (Virtual Metropolitan Area Network tag) qui correspond au tag du « super VLAN » qui transporte d'autres VLANs dont le tag est alors appelé le *inner tag*.

L'utilisation du Q-in-Q implique de pouvoir activer le jumboframe sur les interfaces concernées, car l'ajout de ces 4 octets porte à 1526 la taille d'une trame Ethernet.

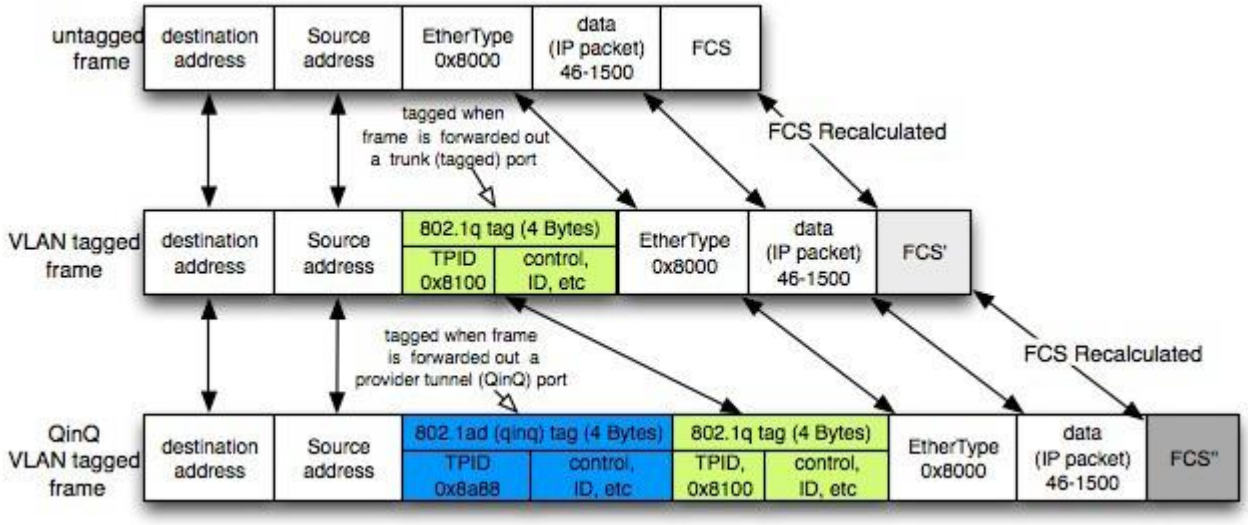


Figure 28 : ajout des 4 octets en en-têtepour le QinQ

Annexe 6 : Fichier d'inventaire

Tableau III : Tableau Excel utilisé pour l'inventaire des versions des switches.

Liste des switchs restant à mettre à jour vers l'iOS 12.2(55)SE4

Bâtiment/Salle	Device Name	IP Address	IOS	Nom de l'image	Switch accès ou distribution	VLAN impactés	Contact client

Fichier vierge pour raison de confidentialité

	Nombres de switches à Upgrader restant:		Document mis à Jour le	

Annexe 7 : Les différents états des ports

Source : http://cisco.goffinet.org/s3/spanning_tree

Cinq états de ports peuvent rencontrés sur un port STP. Chaque état comporte un délai. En voici les propriétés.

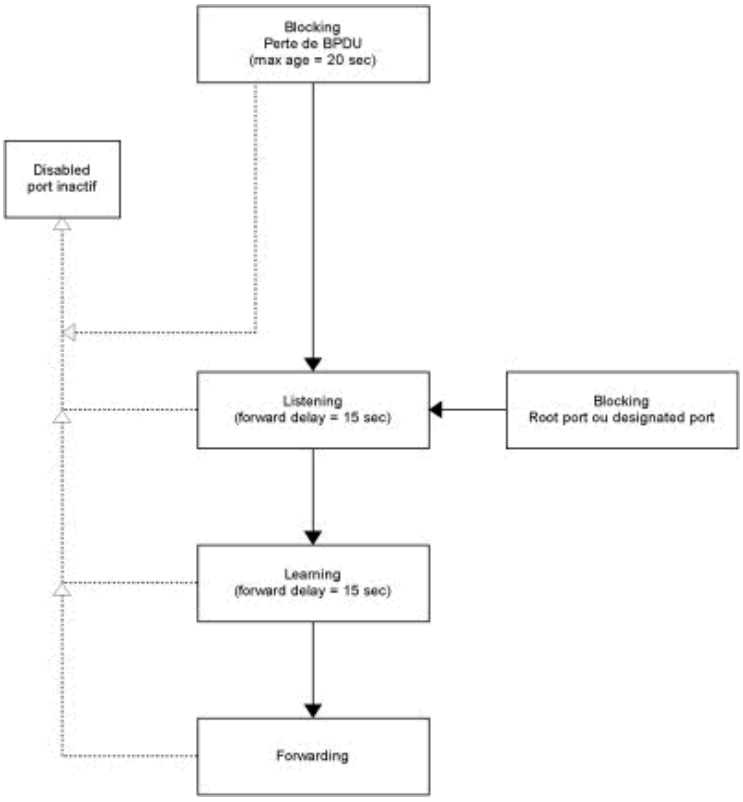


Figure 29: Séquence des états des ports

L'age maximal de 20 secondes par défaut est le temps maximal avec que STP effectue de nouveaux calculs quand une interface ne reçoit plus de BPDUs. Le temps de forwarding de 15 secondes par défaut est le temps de passage d'un état "listening" à "learning" et de "learning" à "forwarding". La fréquence d'envoi de BPDUs Hello est de 2s par défaut.

Etat « Blocking »

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- N'envoie pas de BPDUs reçus de son système
- Répond à SNMP

Etat « Listening »

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

Etat « Learning »

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- Intègre les emplacements de station dans sa MAC table (apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

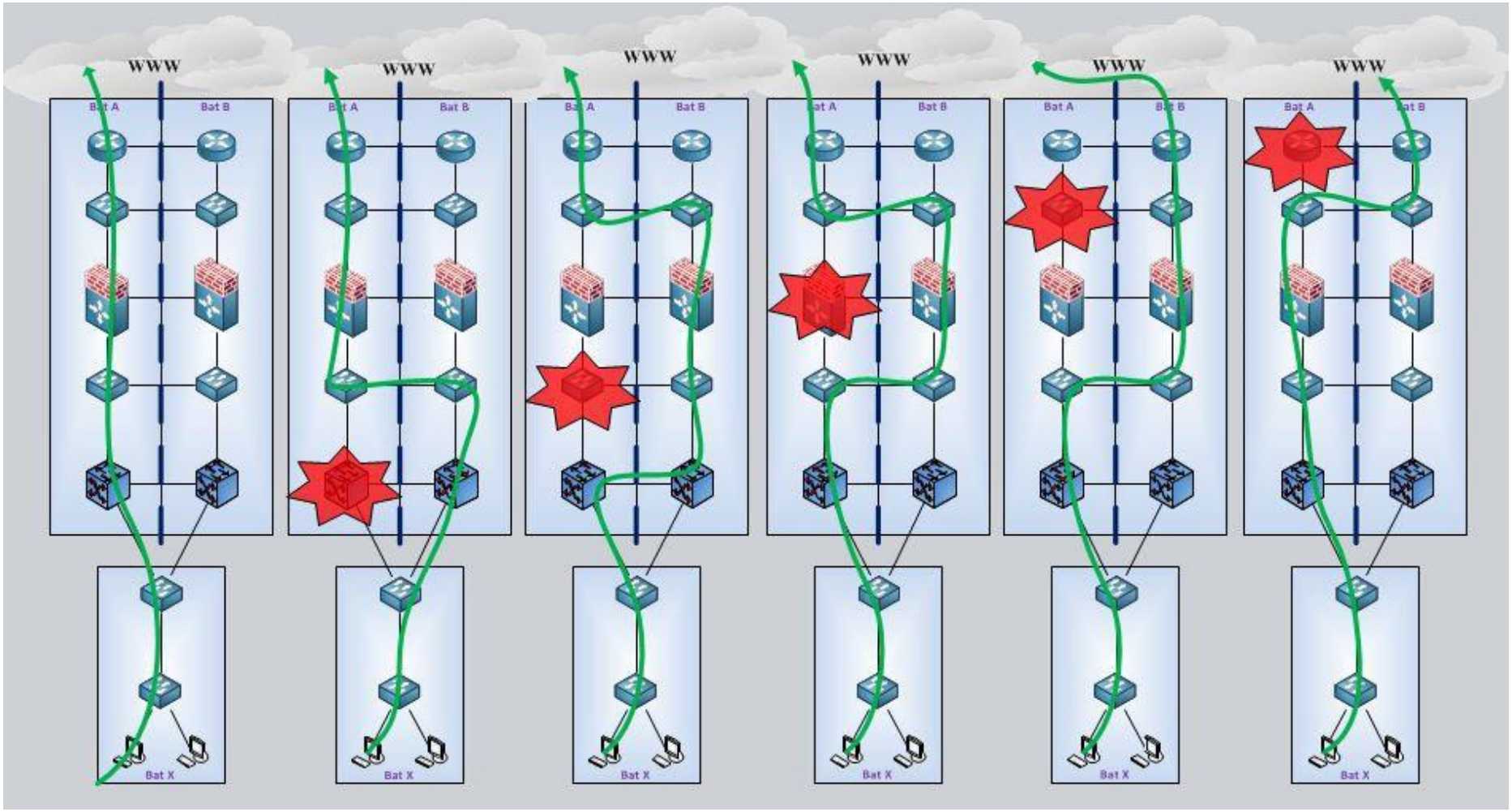
Etat « Forwarding »

- Commute toutes les trames de données venant du segment attaché
- Commute toutes les trames de données venant d'un autre port de transfert
- Intègre les emplacements de station dans sa MAC table (apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

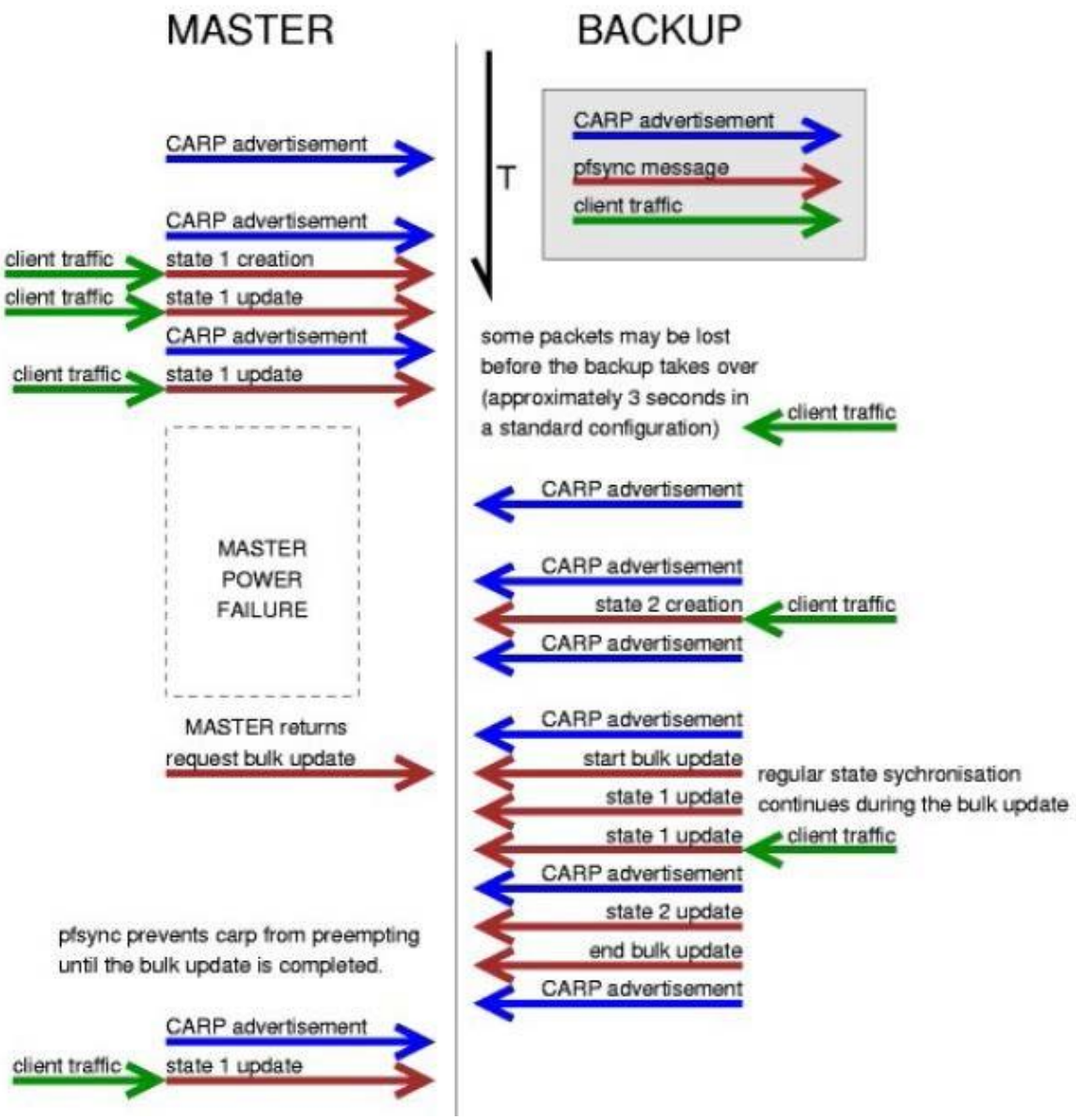
Etat « Disabled »

- Cet état est similaire à l'état « blocking » sauf que le port est considéré physiquement non opérationnel (*shut down ou problème physique*).

Annexe 8 : Scenario de test et résultats obtenus



Annexe 9 : Chronogramme d'un failover CARP + pfsync



Liste des figures

Liste des tableaux

Plan de continuité d'activité réseau et protocoles de redondance.
Mémoire d'Ingénieur C.N.A.M., Toulouse 2012

RESUME

Internet Projet est un réseau particulier, dédié aux équipes projets ayant besoin d'un accès internet. Le nombre de projets pouvant bénéficier des services internet a augmenté considérablement ces dernières années. Vite, trop vite pour avoir le temps de se préparer au pire : une coupure Internet qui paralyse les activités de certains projets pendant une longue période.
Le manque de budget ne permet pas toujours de faire évoluer le réseau informatique pour répondre à des besoins toujours plus nombreux. Pourtant, qu'il touche au domaine financier ou à l'image de l'entreprise, l'impact n'est pas négligeable. Aussi, il et important d'apporter une solution permettant de répondre à cette problématique : un Plan de Continuité d'Activité.
Sa construction a vu émerger un plan d'action à mettre en œuvre afin de garantir une continuité de service en cas de panne. À partir de ce plan, en a découlé ce projet, qui concerne la mise en œuvre d'une architecture redondée.

À chaque couche du réseau, un mécanisme s'appuyant sur des protocoles spécifiques a été mis en place afin de garantir la suppression des points de panne unique et offrir une haute disponibilité au réseau Internet Projet.

Mots clés : Continuité, activité, réseau, informatique, PCA, redondance, protocoles.

SUMMARY

Internet Project is a particular network, dedicated to project teams who need internet access. The number of projects eligible for internet services has increased significantly in recent years. Fast, too fast to have enough time to prepare for the worst: a cut which paralyzes the Internet activities of certain projects for a long time.
The lack of budget does not always allow to developp the IT network to meet growing needs. However, it affects to the financial area or image of the company, the impact is not negligible. Also, it is important to provide a solution to address this problem: a Business Continuity Plan.
From its construction has been emerged an action plan to implement to ensure continuity of service in case of failure. This plan resulted into this project, which involves the implementation of a redundant architecture.

At each layer of the network, a mechanism based on specific protocols, has been put in place to ensure the elimination of single points of failure and provide high availability to the Internet Project.

Key words : Continuity, business, network, IT, PCA, redundancy protocols.