Administration de l'infrastructure du Système d'Information

6, rue du Manège
54000 NANCY
FRANCE

pascal@rodmacq.com
www.rodmacq.com

00 33(0)3 83 35 39 33

Pascal Rodmacq - Juin 2006

Introduction -1

- Ce qu'on attend communément de l'administrateur
- Image du rôle d'administrateur
- Les héritages de la fonction administration
- Tâches prêtées à l'administrateur

Ce qu'on attend communément de l'administrateur

Installer

- les équipements réseaux
- les systèmes d'exploitation
- les applications

Assurer le bon fonctionnement de certains processus basiques

- authentification
- système d'impression
- messagerie
- accès à internet

Traiter des événements à pattern pré-établi

- arrivée/départ d'utilisateur
- création/suppression de données (fichiers, répertoires)
- modification de permissions
- déplacement d'utilisateur (sur site, inter site)
- installation d'un poste de travail, d'une imprimante …

Traiter des événements imprévus

- panne d'un poste de travail, d'une imprimante, d'un serveur …
- virus, ver …

Assister les utilisateurs

- login, impression, utilisation de logiciel, droits, restauration,

Image et contenu du rôle d'administrateur

La rôle d'administrateur apparaît donc comme extrêmement confus et tout à fait de-structuré.

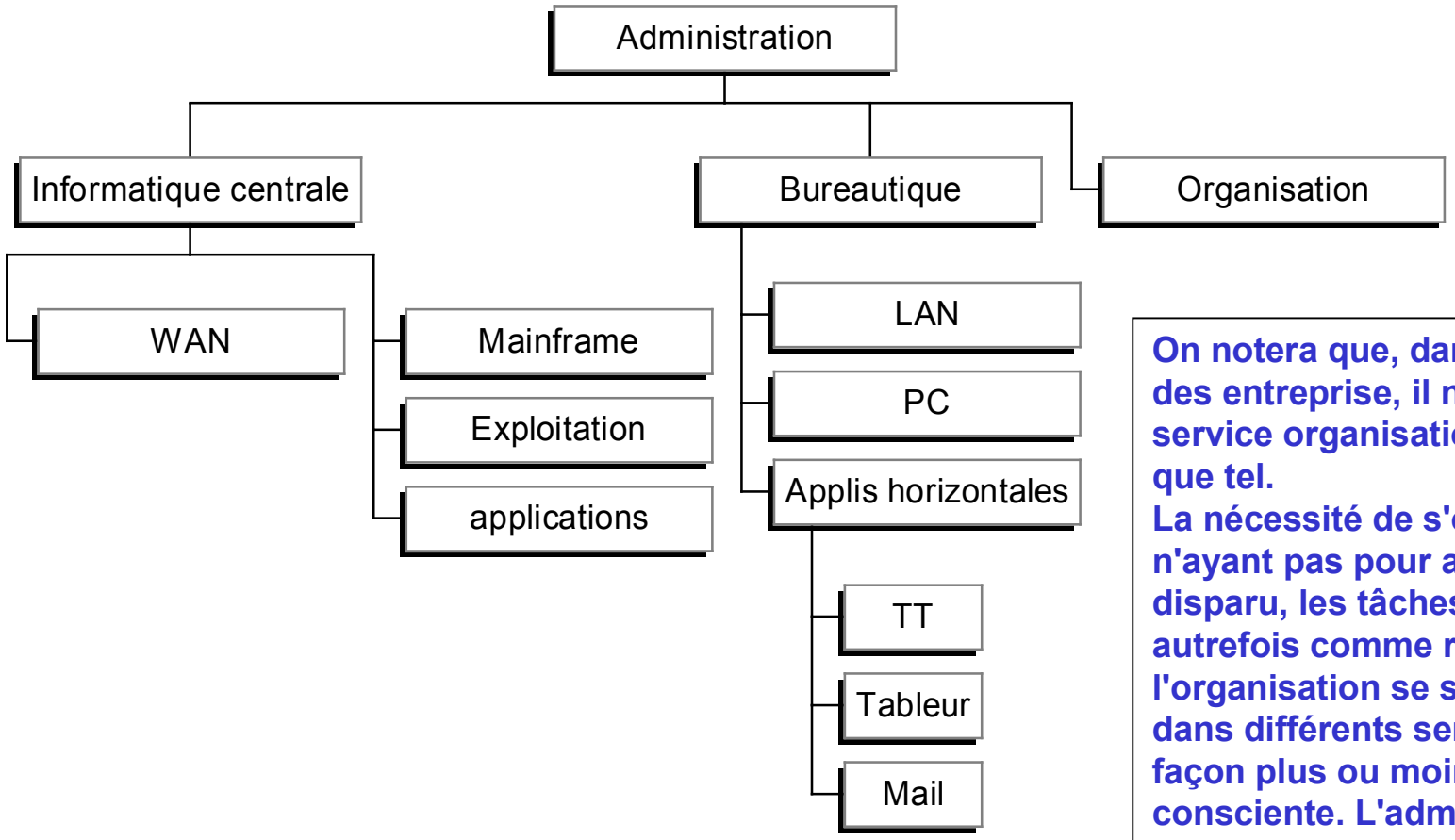
Le rôle est souvent décliné :

- administrateur systèmes, réseaux (ou les 2)
- administrateur NT, NetWare, Unix
- administrateur Exchange, Notes, GroupWise
- administrateur de bases de données …
- administrateur DNS
- administrateur Citrix
- administrateur NAS/SAN

Enfin, quand il n'est pas décliné, ça veut dire qu'il faut s'occuper de tout !

Dans ce cours, nous nous attacherons à définir un cadre cohérent et opérationnel à la fonction d'Administration de l'infrastructure du Système d'Information, de façon à disposer de clefs pour l'organisation et le suivi de cette fonction au sein de l'entreprise.

Les héritages de la fonction administration



On notera que, dans la plupart des entreprise, il n'y a plus de service organisation en tant que tel.
La nécessité de s'organiser n'ayant pas pour autant disparu, les tâches identifiées autrefois comme relevant de l'organisation se sont diffusées dans différents services de façon plus ou moins consciente. L'administration des SI en a hérité une part, souvent importante.

Fonctions prêtées à l'administrateur

Les fonctions prêtées à l'administrateur sont devenues extrêmement étendues et variées, on peut les trier en fonction de l'analyse précédente.

Certaines sont héritées de ce qu'on appelle encore l'exploitation :

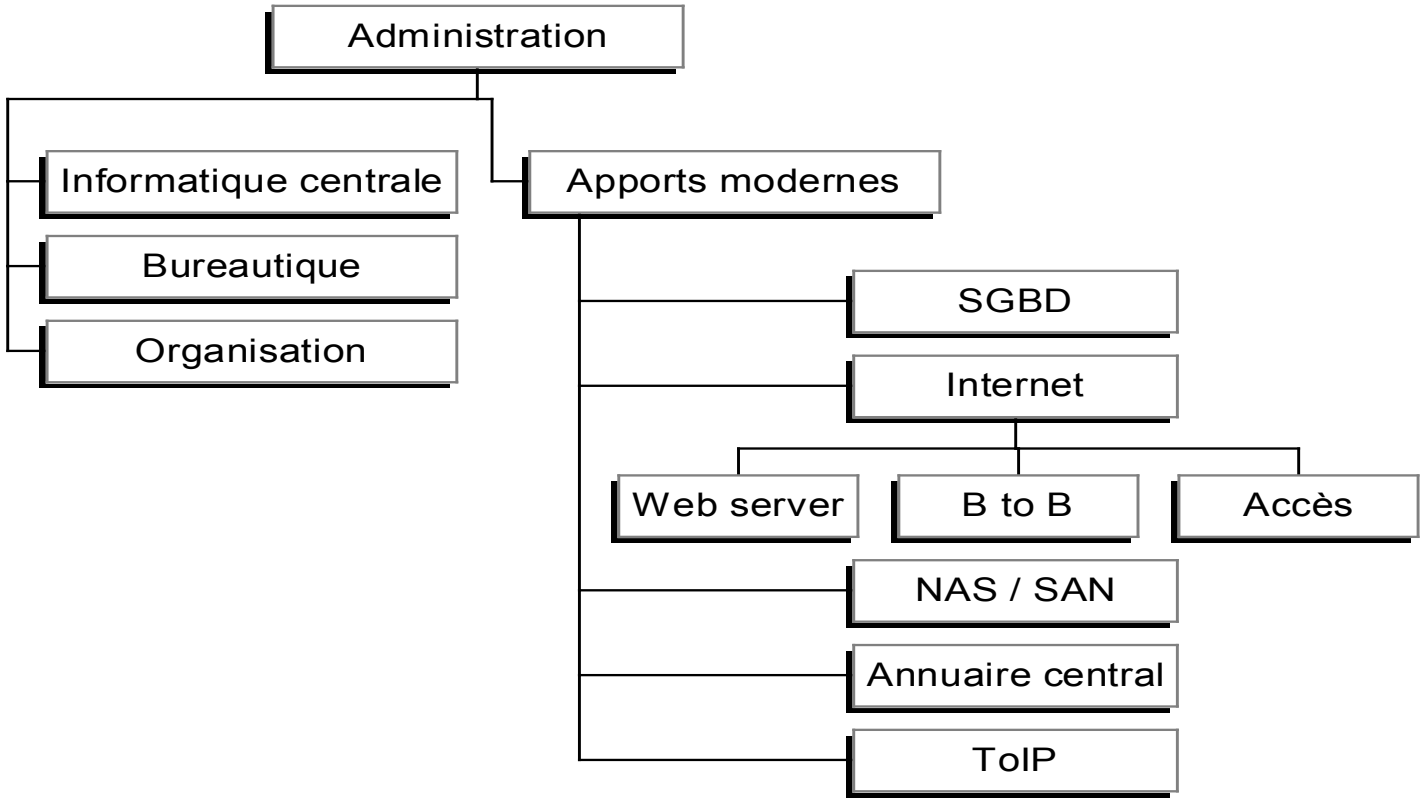
- centrées sur la gestion des serveurs centraux
- surveillance des paramètres d'exploitation : occupation disques / CPU
- surveillance des process systèmes et applicatifs
- maintenance système : patch sauvegardes systèmes
- maintenance applicative : mise en production, sauvegarde données
- supervision WAN

Certaines sont héritées de la bureautique et des LAN :

-gestion du parc matériels : postes de travail, imprimantes
- maintenance des postes de travail
- installation/distribution de logiciels client
- fonctionnement du LAN (permettre à une station de communiquer)
- gestion des comptes utilisateurs
- gestions des ACL
- support aux utilisateurs

Les apports modernes

Les apports modernes sont extrêmement nombreux et posent un véritable challenge sur la fonction d'administration du Système d'Information.
Le risque est précisément que chacun de ces domaines soit traité comme un silo, sans qu'on remette en cause les schémas existants, s'interdisant les bénéfices de l'acquisition en terme d'allégement de la charge administrative.



Introduction -2

- **Définitions**
- **Modes de fonctionnement de l'organisation**
  - **Projet**
  - **Crise**
  - **Administration (normal)**

Définitions

Système d'information : inclus tous les objets - et les relations entre ces objets – qui concourent à créer, rendre accessible, permettre la mise-à-jour des informations utilisées par l'entreprise pour son fonctionnement.

Le système d'information n'inclus pas seulement des objets informatiques, toutefois dans ce cours nous ne considérerons que ceux-ci.

Administrer : effectuer les actions nécessaires pour maintenir le système d'information dans un état de fonctionnement satisfaisant. C'est à dire gérer les changements qui affectent le SI de telle sorte qu'ils ne le dégradent pas.

Niveau de satisfaction : difficile à définir par des critères valués. Les indicateurs techniques chiffrés ne sont qu'une petite composante du niveau de satisfaction, les mesures de niveau plus élevé sont à inventer pour chaque organisation en fonction des priorités de son métier.

Mode de fonctionnement - projet

Gestion du changement : l'administration vise à gérer un certain niveau de changement, le changement prévisible, correspondant à des événements courants qui ne remettent pas en cause l'architecture générale du système.

Mode Administration / mode Projet : les changements qui remettent en cause l'architecture du système se gèrent en mode projet, ils sortent du cadre de l'administration.

Face à un événement, on doit être capable de tout de suite savoir si sa gestion relève du mode administration ou implique la mise en place d'un autre type d'organisation.

Ce n'est pas toujours évident, on a tendance dans les entreprises à mettre en place de nouveaux produits avec l'organisation d'administration, ce qui est une erreur.

Mode de fonctionnement - crise

Mode Administration / mode crise : certains événements remettent radicalement en cause le fonctionnement du système d'information de façon brutale et imprévisible.

La gestion de ce type d'événement doit se faire par un mode de fonctionnement spécifique qui implique une structure de communication et de décision les plus directs possibles.

Il y a bien lieu de comprendre que le mode de fonctionnement habituel de l'administration n'est pas adapté à gérer ce type d'événement, on voit souvent pourtant, des entreprises laisser le service chargé de l'administration gérer, par exemple l'incendie d'un site avec leur structure de décision et de fonctionnement habituelle.

Un changement peut donc relever d'au moins trois modes distincts de fonctionnement :

Administration **Projet** **Crise**

Administration du SI : Quoi ? Comment ?

Objets

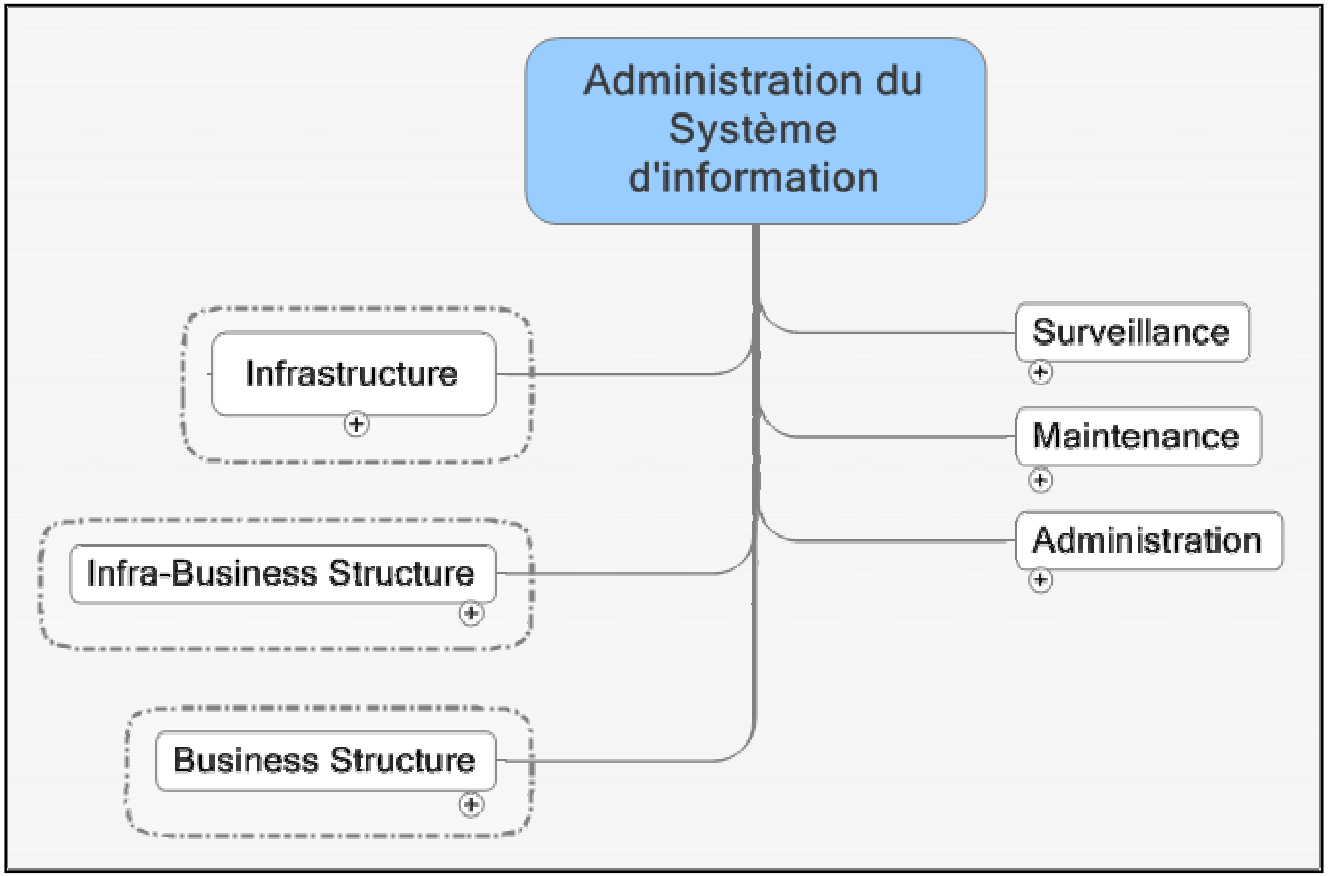
- Infrastructure
- Infra-business structure
- Business structure

Nature des tâches

- Surveillance
- Maintenance
- Administration au sens strict

Quoi ? Comment ?

L'administration est une combinaison entre d'une part une nature de tâches (à droite) et les cibles sur lesquelles s'appliquent cette nature de tâche (à gauche)
Encore une fois, la réflexion sur la structuration du SI est fondamentale.



	Objets Physiques	Objets Logiques	Concepts	Niveau SI
1	Connecteurs cables baies hubs switchs	Site LAN Campus	Topologie Plan Bande passante	Infra
2	Adaptateurs Hubs Bridges Switchs	MAC Trame CSMA 802.x STP QoS ARP DLC	Espace de collision et de broadcast VLAN	
3	Routeurs Firewall Proxy PABX IP	TCP SNA IPX RIP OSPF BGP MPLS VPN NAT SOCKS SIP RTP	Espace d'adressage Adresses privées Adresses publiques Opérateurs (telcos) AS / Frontière	Structure
4	Serveurs d'infrastructure	DHCP DNS SLP NTP NDS AD LDAP ZenWorks SMS SMTP POP IMAP SNMP	Gestion de noms Authentification Représentation des objets du réseau Messagerie	Infra Business Structure
5	Postes de travail	OS Stations Données Applications	Environnement utilisateur / Service	Business Structure

Surveillance / Maintenance / Administration

Surveiller consiste à :

Observer
Confronter ses observations à des standards
Alerter si les observations sortent des standards

Cela signifie qu'il faut avoir défini des standards, savoir quoi observer, avoir défini une procédure d'alerte.

Maintenir consiste à :

Prendre conscience d'une opération de correction nécessaire
Définir l'opération de correction
Mettre en œuvre les corrections

La maintenance est, en général, actionnée par la surveillance, l'occurrence des événements (sinon leur nature) est imprévisible. L'opération de maintenance en elle même n'est pas forcément standard, les situations peuvent être très variées. C'est pourquoi, il est préférable de définir des politiques de maintenance au sein desquelles vont s'inscrire les actions.

Administrer consiste à :

Définir les événements types normaux à caractères récurrents qui vont affecter le SI.
Définir un traitement type associé à ces événements types, les événements étant de nature prévisible et d'occurrence élevée, il est généralement intéressant d'en automatiser le traitement.

Croisement objet / action – à compléter

	Surveiller	Maintenir	Administrer
Infrastructure	Environnement Baseline réseau Baseline routeur	Gestion des pannes matériels (actif, routeur, serveur, imprimantes) Maj firmware	Accès armoires, switch, routeur Brassage Repérage VLAN Releases firmware
Infra-structure business	Process DHCP DNS WINS NTP SGBD ANNUAIRE	OS : patchs maj Services : patchs maj	Adresses DHCP Releases Sauvegardes Licences
Business Structure	Baseline serveur Transactions (baseline) Point de vue user Satisfaction	Applications : maj Données : organisation, permission, backup / restore	Utilisateurs Permissions Données Sécurité

Approche de l'administration par couche

- infrastructure
- Infra-business structure
- Business structure

D’une manière générale, au niveau de l’infrastructure

On suppose que l’on dispose d’une infrastructure documentée correspondant à une architecture claire, sans ces préalables, il n’y aura pas de bonne surveillance / maintenance / administration possibles.

Maintenir le système en conformité avec son design

Contrôler les modifications et notamment ne pas admettre de modifications qui viennent en contradiction avec le design existant (suppose qu’il faut connaître les choix / principes sur lesquels repose son design)

Mettre à jour la documentation.

Répondre aux événements dégradants

Traiter les pannes, intervenir pour assurer le fonctionnement malgré la panne, ceci doit être prévue dans la politique de maintenance définie et peut entraîner, un re-câblage, une simple demande de remplacement de la pièce défectueuse (le design assurant la redondance), la mise en service d’un équipement en spare …

La maintenance consiste surtout à surveiller la conformité vis-à-vis de standards pré-établis et de répondre aux événements imprévus.
Le traitement de ce type d’événement n’est à priori pas adapté à l’automatisation.

Maintenance de la politique de maintenance

Il faut définir une politique de maintenance. (Voir I141) et cela veut dire qu'il y correspond des écrits dans l'entreprise, des principes affichés, connus, répétés.
C'est au service chargé de l'administration du SI de gérer cet aspect.

La politique de maintenance définit des priorités et s'appuie sur des choix. Ces choix servent d'entrée au design, ils sont éventuellement arbitrés par des questions de coûts.

Il est bon de rappeler l'importance du design : c'est le design, en incluant une certaine redondance, qui peut seul garantir le niveau de résilience souhaité pour tout équipement dont le délai de remise en service ne saurait autrement être ramené en dessous de 2/3 heures (en mettant les choses au mieux).

Ensuite, tout équipement, en fonction de sa place au sein du design pourra se voir affecter une classe de criticité (on a pu voir qu'un design hiérarchisé facilite cette tâche) à laquelle la politique de maintenance associera une réponse adaptée.
Cette réponse suppose un certain nombre de choses en terme d'organisation, de compétences présentes ou non, de réponses des fournisseurs, de prix, de niveau de design, toutes choses qui ont été validées la première fois au stade de la conception.

Ceci dit, ces paramètres peuvent varier et impliquer des aménagements, soit de la politique de maintenance elle même (ce qui devrait rester rare), soit (ce qui peut être plus fréquent) des réponses prévues (traitement des incidents).

D'où la maintenance de la politique de maintenance !

	Objets Physiques	Objets Logiques	Concepts	Niveau SI
1	Connecteurs cables baies hubs switchs	Site LAN Campus	Topologie Plan Bande passante	Infra
2	Adaptateurs Hubs Bridges Switchs	MAC Trame CSMA 802.x STP QoS ARP DLC	Espace de collision et de broadcast VLAN	
3	Routeurs Firewall Proxy PABX IP	TCP SNA IPX RIP OSPF BGP MPLS VPN NAT SOCKS SIP RTP	Espace d'adressage Adresses privées Adresses publiques Opérateurs (telcos) AS / Frontière	Structure
4	Serveurs d'infrastructure	DHCP DNS SLP NTP NDS AD LDAP ZenWorks SMS SMTP POP IMAP SNMP	Gestion de noms Authentification Représentation des objets du réseau Messagerie	Infra Business Structure
5	Postes de travail Serveurs fichiers app.	OS Stations Données Applications	Environnement utilisateur / Service	Business Structure

Administration du niveau Infrastructure

Pascal Rodmacq - Juin 2006

Administration niveau 1

Objets Physiques	Objets Logiques	Concepts	Documents
Connecteurs câbles baies	Site LAN Campus	Topologie Environnement Bande passante	Design/Plans Repérage Procédures d'accès

Surveiller l'environnement (reste conforme aux présupposés)

Gérer les accès aux armoires

Maintenir la présence / cohérence du repérage

Maintenir le brassage à ce qui est nécessaire

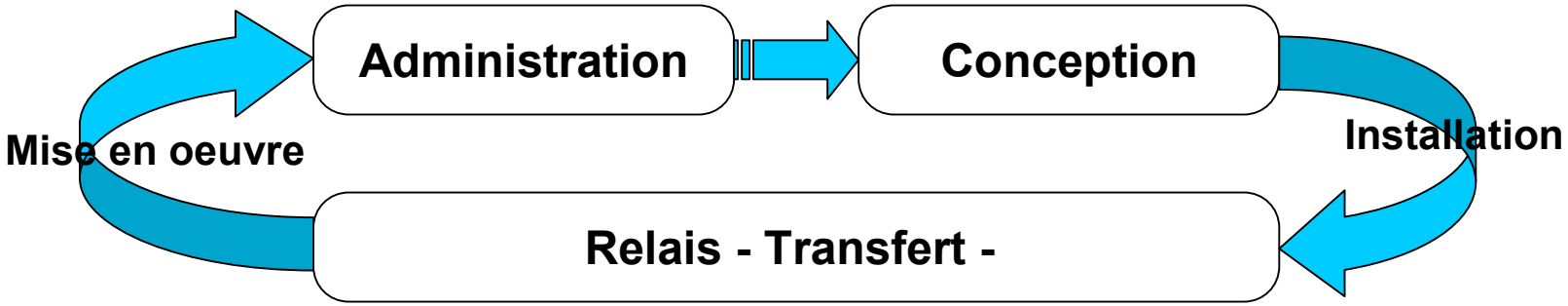
Documentation

Documents à gérer :

- Plans des locaux avec emplacements des prises
- Plans du détail des armoires de câblage
- Garantie constructeur
- Coordonnées prestataire câblage
- Procédures d'accès aux armoires

Enseignement

On peut noter à ce niveau, et ce sera en fait général, que l'administration doit s'appuyer sur les résultats de la phase de conception et sur les documents de la mise en place initiale.
Il doit y avoir une phase passage de témoin, relais, entre la conception, l'installation puis la mise en œuvre et l'administration.



Surveillance - Evénements

Suivi – Best practices - Veiller à ce que :

- le nombre d'utilisateurs reste compatible avec le nombre de prises disponibles plateau par plateau. Indicateur : nombre de prises / nombre d'utilisateurs.

- on utilise les cordons correspondant à la norme de câblage

- on ne brasse que ce qui est nécessaire (pour des raisons de sécurité, contrôle, facilité de diagnostic le cas échéant – à moins qu'on implante un protocole de contrôle d'accès au réseau comme 802.1x)

- on maintienne un système de repérage cohérent et à jour (surtout lorsqu'on a des VLANs)

- l'environnement ne soit pas sauvagement modifié (lieu rendu accessible au public, électro-magnétisme, volumes modifiés …) Notez que ces paramètres sont censés avoir été pris en compte à la conception et constituent des pré-supposés.

Procédures pour traiter les événements :

- **Ajout suppression d'équipement sur un plateau (ajout d'une imprimante, mouvement d'utilisateur …)**

- Accès aux armoires de brassage

Administration au niveau 2

Objets Physiques	Objets Logiques	Concepts	Documents
Adaptateurs hubs switchs Bridges	MAC Trame CSMA 802.x STP QoS ARP DLC	Espace de collision et de broadcast VLAN	Politique de maintenance Design/Plans Inventaire

Surveillance : baseline par espace de broadcast

- **Bande passante**
- **Bande passante ventilée par protocole**
- **Confrontation des mesures aux baseline**

Gérer les événements en conformité avec la politique de maintenance.

Gérer les E/S de matériels

Maintenir la documentation et l'inventaire à jour

Inventaire et documentation

Les documents qui ont été créés à la conception et à l'implantation doivent être pris en charge et éventuellement complétés, aménagés par et pour l'administration.

Schémas

- **Schéma physique du LAN : équipements (avec leur adresse), liaisons, port**
- **Schéma logique du LAN : mise en évidence des espaces de broadcast et ou des VLANS**
- **Schéma logique du LAN : mise en évidence des instances STP avec repérage des root bridge et root port(s) sur ces équipements.**

Inventaire

-**Matériel : ID, modèle, Firmware, nombre et type de ports,**
- **VLAN : ID, description : pourquoi ce VLAN ?**
- **Technologies supportées : identifier le matériel par classe de technologie supportée (génération) dans le but notamment de gérer l'hétérogénéité induite par l'introduction de matériel de nouvelle génération.**
- **Applications utilisant un protocole non routable => surveiller leur agonie et la favoriser le cas échéant..**

Organiser la sauvegarde des configurations

- **Convention de nommage (à écrire et à respecter scrupuleusement)**
- **Emplacement défini**
- **Implique souvent l'usage de tftp**

Documentation et traitement des événements

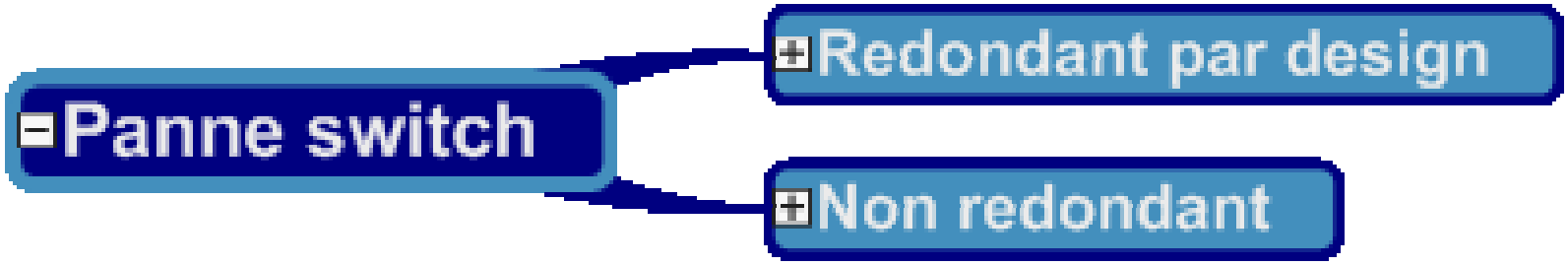
Les outils d'organisation des connaissances peuvent servir pour organiser une documentation créée avec des outils disparates et pour créer des procédures par arbres de décision.

Imaginons l'événement : panne switch. Le traitement correct de cet événement implique de pouvoir répondre à une série de questions dont les réponses ont été obligatoirement générées, soit au moment du design, soit au moment de l'installation / mise en service et au cours des éventuelles opérations de maintenance qui ont pu avoir lieu depuis.

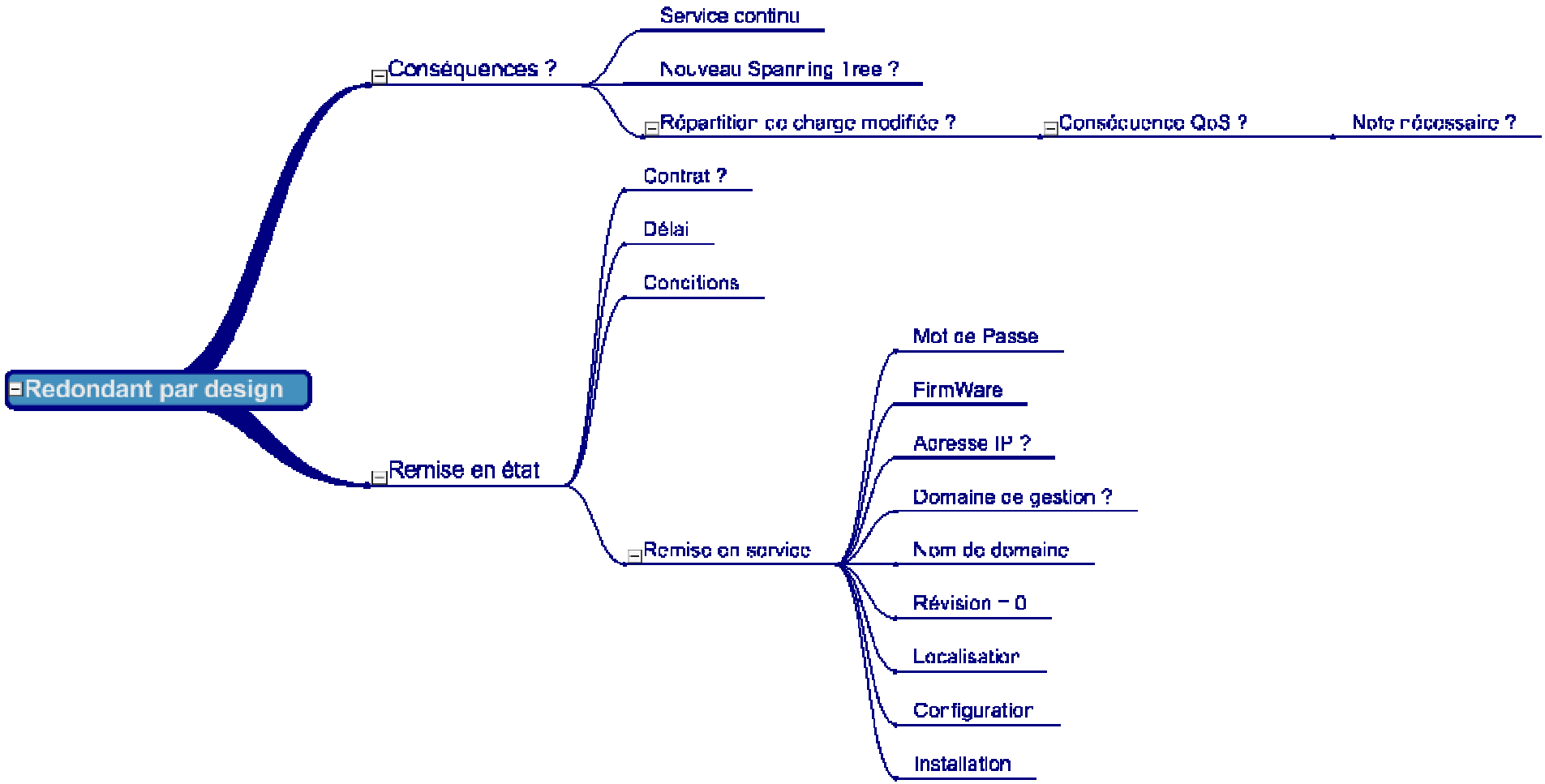
- **Connaître le rôle du switch dans l'architecture**
- **Redondé ou non ?**
- **Supportait-il des ports Root pour des spaning tree ?**
- **Niveau de firmware ? (sauvegarde ? Où ?)**
- **configuration (sauvegarde ? Où ?)**
- **VLAN, trunking ? De quel type ? ISL ? 802.1q ? Mode ?**
- **appartient à un domaine ?**
- **rôle dans le domaine ?**

Il peut s'avérer excellent de créer un arbre de décision pour chaque événement type d'importance. C'est d'une part un bon moyen d'audit de son niveau de documentation, une façon de l'organiser (l'information) et de la compléter, si elle ne l'est pas déjà, et enfin une aide précieuse pour gérer l'événement.

Arbre de décision : panne switch



Arbre de décision
panne switch
1- Redondant



Arbre de décision panne switch 2- non redondant

Surveillance niveau espace de broadcast

Etablissement de baseline réseau :

Une baseline est une mesure de référence à laquelle on se référera lorsque l'on voudra s'assurer de la normalité du trafic. Une baseline se remet à jour si les conditions d'exploitation changent (par exemple : significativement plus d'utilisateurs, ajout d'une application …)

Le principe est donc d'établir des mesures de référence dans une situation que l'on considère comme normale. Il peut y avoir une série de mesure par type de période (période creuse, période de pointe, période standard, fin de mois …)

La définition des périodes dépend de chaque entreprise, si le mode d'exploitation est très homogène 1 ou 2 mesures peuvent suffire, si l'entreprise connaît des pics d'activité réguliers, une mesure pendant ces pics définira la notion de pic normal hebdomadaire, mensuel, …

En terme de surveillance, on va de temps à autre refaire le même type de mesure, dans des moments similaires que l'on comparera à la baseline pour vérifier qu'on reste bien dans les clous.

En cas de soupçons de charge anormale, on refera des mesures qu'on comparera avec la baseline.

Surveillance niveau espace de broadcast

Etablissement de baseline réseau (suite)

Ou ?

Si on a un nombre d'espace de broadcast raisonnable, une baseline par broadcast. Correspond au nombre de segments dans un réseau à média partagé et au nombre de VLANs dans un réseau switché.
Si on a un grand nombre de segments ou VLANs, il faut faire preuve de discernement … et utiliser les fonctionnalités spécifique des switchs pour ponter le trafic sur un port particulier.
Il est de toute façon obligatoire de documenter les endroits où on prend les mesures et l'endroit où on les stocke !

Quoi ?

Bande passante utilisée
% de broadcast (paquets / Octets)
% de multicast (paquets / Octets)
Distribution des paquets en fonction de la taille
% de trames erronée

Administration des VLANs

Au niveau 2, l'administration des VLANs est une des tâches les plus lourdes dès que le réseau atteint une certaine taille.

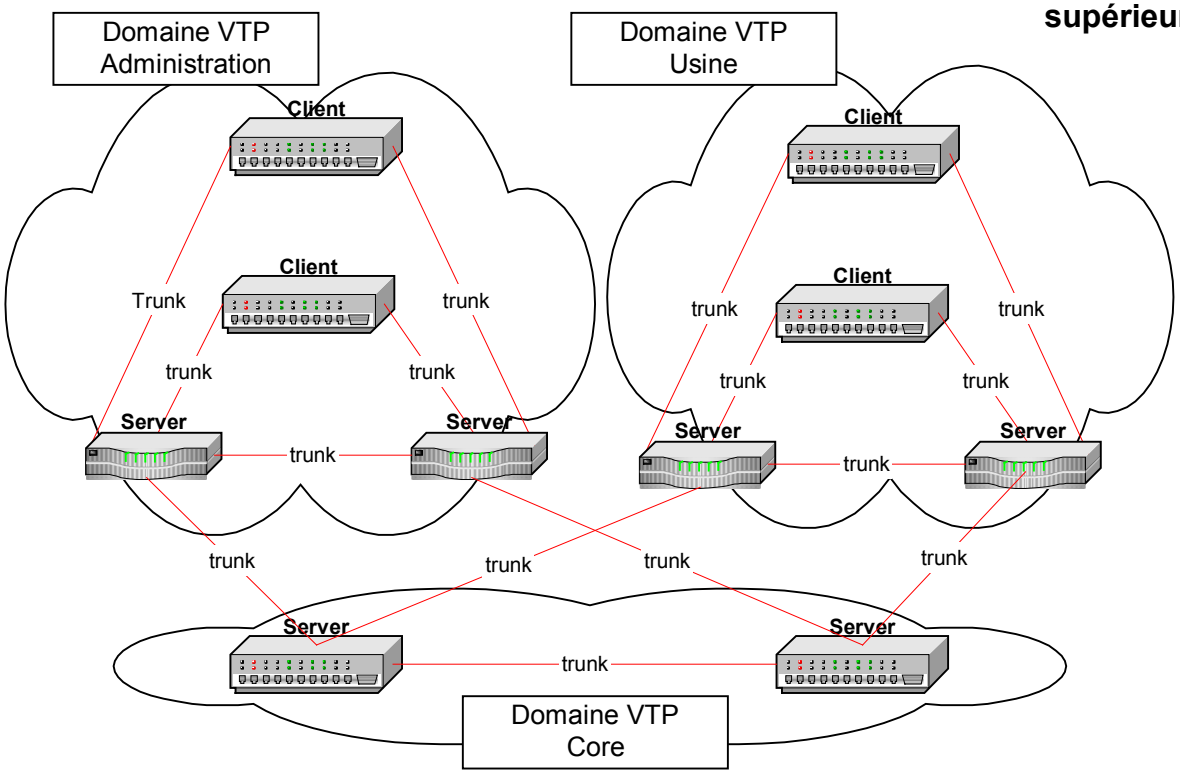
C'est un type de tâche pour lequel l'effet d'échelle est très important, elle n'apparaît pas ou peu dans un petit réseau mais doit être absolument dominée dans un réseau important.

Il est clair que le nombre de combinaisons croît exponentiellement en fonction du nombre de switchs et du nombre de VLANs.

Pour faciliter le travail d'administration, les constructeurs proposent des notions de «domaines» d'administration, cad que les modifications faites sur un switch d'un domaine se répercutent sur les autres switchs du même domaine (VTP VLAN Trunking Protocol chez CISCO)

Ce type de protocole implique d'avoir à gérer : les noms de domaines, et la notion de switch serveur (sur lesquels on peut créer/supprimer un VLAN) et de switch client qui ne peuvent qu'ajouter/supprimer des ports à un VLAN déjà existant. Il y a aussi un certain nombres de conditions : VTP ne passe que sur des liens de type trunk et tous les switchs d'un même domaine doivent être adjacent.

VTP : exemple de configuration



Insertion d'un nouveau switch : on peut écraser la configuration existante de l'ensemble du domaine avec un numéro de révision supérieur au numéro en cours

Les domaines ne sont pas « transitifs » tous les switchs d'un domaine doivent être contiguës, ce qui oblige en pratique plusieurs domaines dans un design où le DB sont isolés par des routeurs.

Rentabilité globale des outils

Evaluer overhead / gains

L'exemple précédent nous montre que l'introduction d'un outil de gestion entraîne ipso-facto un certain overhead, en terme de coût, de disponibilité et de complexité.
Pour que l'outil soit rentable, il ne faut pas que l'overhead induit soit supérieur aux gains reçus.

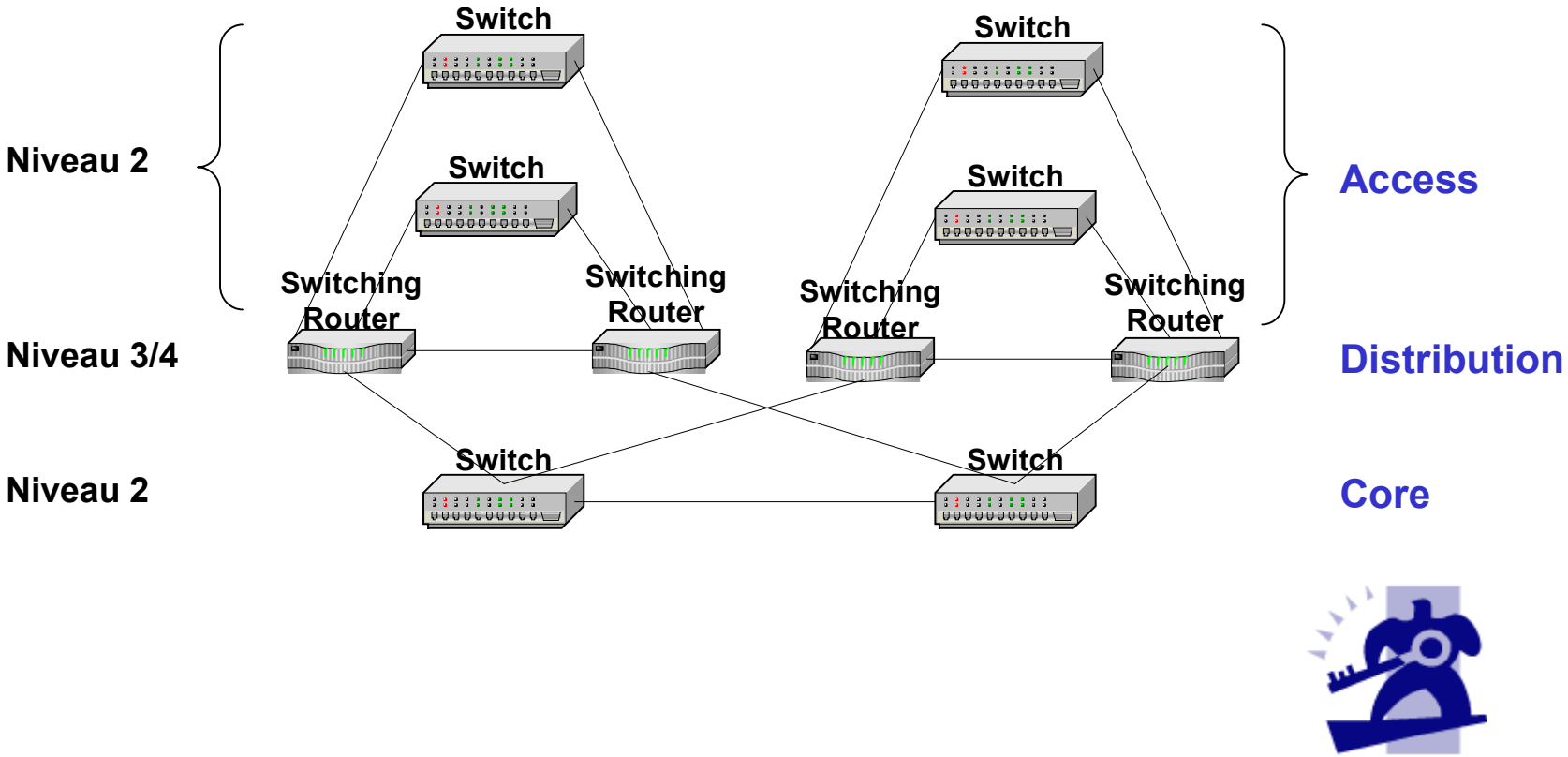
Gérer le pic de la mise en place

De plus, la mise en place requiert nécessairement un surcroît ponctuel de travail qui doit être pris en compte et managé.
Attention dans ces circonstances au fournisseur miracle qui mettra un système en place sans le transfert de compétences et vous rendra totalement dépendant pour la moindre action ultérieure.

S'acculturer aux technologies avant tout

Il est fondamental de s'acculturer à la technologie mise en œuvre avant tout choix, en général, personne ne peut penser à votre place. Les fournisseurs vendent normalement une «solution», cad quelque chose de pré-pensé !
Enfin, seules les tâches bien maîtrisées conceptuellement devraient faire l'objet d'une automatisation.

Exemple de design à 3 niveaux (campus)



Administration Niveau 3

Objets Physiques	Objets Logiques	Concepts	Documents
Routeurs **Firewall Proxy** **PABX IP**	**TCP SNA IPX** **RIP OSPF BGP** **MPLS VPN** **NAT SOCKS** **SIP**	**Espace d'adressage** **Adresses privées** **Adresses publiques** **AS / Frontière** **Opérateurs (telcos)**	**Plan d'adressage** **Schémas logiques du réseau et des accès extérieurs** **Inventaires** **Définition des règles en clair.**

Information/documents à maintenir :
- Plan d'adressage
- Adresse des équipements clefs (Routeurs, firewall, proxy, PaBX)
- Espace d'adresses publique
- Règle de firewalling

Surveillance :
- Tables de routages
- Hit sur les règles, log des firewall
- Etat des routeurs

Documentation du niveau 3 à maintenir

Schéma global du WAN :

- identifier et schématiser les différents AS, les protocoles de routage au sein d'une AS et entre AS, les numéros d'area (OSPF IS-IS)
- identifier les routeurs de structure, leur rôle vis-à-vis des aires (OSPF IS-IS)
- identifier firewall, proxy.
- S'il y a certaines particularités dans votre réseau, détaillez les sur un schéma à part.

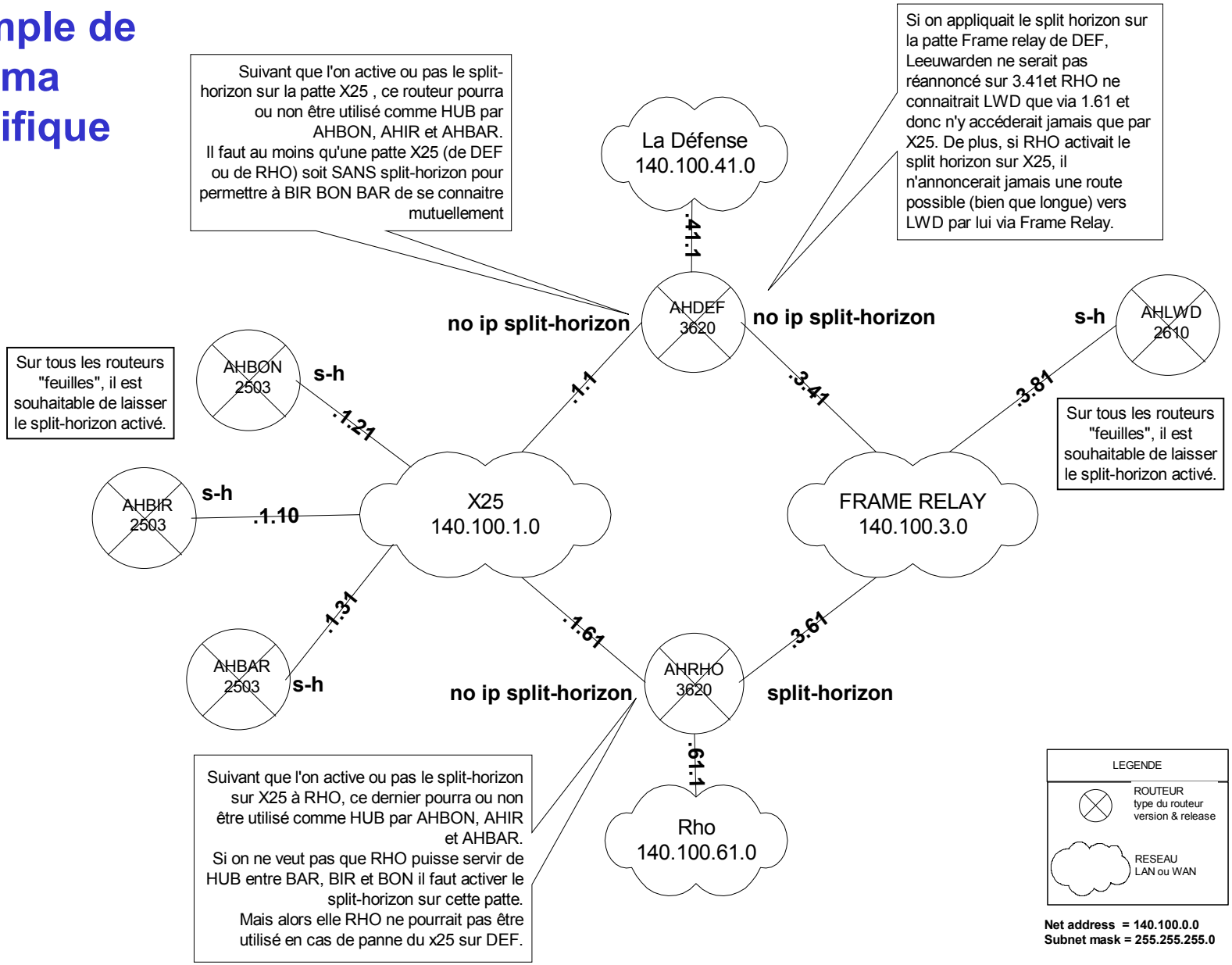
Site par site

-Liste des subnets utilisés
- Par subnet : adresse, masque, Gateway, @DHCP, @DNS
- La liste des routeurs avec version de firmware / logiciel / interfaces
- les liens de backup (ISDN par exemple : nombre et numéro)
- la ligne de télémaintenance RTC (numéro)

Inventaire des routeurs

Model / version de firmware / logiciel / interfaces / accès / affectation (site)
Id contrat de maintenance

Exemple de schéma spécifique



Modèle d'affectation d'adresse

Plan d'affectation d'adresses pour plage de 8 bits

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		Scope DHCP actif														
1																
2																
3																
4																**79**
5	**80**	Scope DHCP secours														
6																
7																
8																
9																**159**
A	**160**	Réservations addresses (imprimantes)														
B																
C																**207**
D	**208**	Adresses fixes (serveurs)														
E																**239**
F	**240**	Actif réseau													**GW**	

Il est important de définir quelques tailles types de blocs d'adresses (par exemple : 7, 8, 9 bits) et de définir par plage un modèle d'affectation comme ci-dessus. Les adresses seront toujours affectées par blocs d'une des longueurs spécifiées et respecteront toujours un modèle d'affectation pré-établi.

Surveillance niveau 3

Etablissement de baselines

Sur les principes vus au niveau 2, on définira un certain nombre de baseline.
J'insiste : la baseline est votre meilleure alliée en situation de troubleshooting !
Vous pouvez utiliser les mêmes moments que ceux définis pour la baseline de niveau 2.

Objectifs des mesures

A ce niveau, on pourra s'intéresser :
- au trafic de bout en bout sur le LAN
(client / serveur, serveur / routeur)
pour pouvoir mesurer la latence totale LAN
- aux échanges de et vers l'extérieur (LAN WAN), ce qui arrive sur la patte WAN du routeur, ce qui arrive sur la patte LAN du routeur.
- aux échanges routeur – routeur à travers le WAN

Cibles : routeurs

Si les équipements réseaux sont sous la responsabilité d'un opérateur, on doit lui demander l'établissement des baseline et la possibilité de refaire le même scénario de mesure à la demande. (à négocier avant la signature …)

Surveillance niveau 3

Ce qu'on peut mesurer

Routeur

Mémoire
buffer
le débit en paquets/sec et en Ko/sec en entrée et en sortie
les 50 nœuds les plus appelés en entrée et en sortie
une ventilation par protocole en paquets / en Ko sur la période
Etat de la table de routage
Hits sur access list

Firewall

nombre de sessions ouvertes en entrée et en sortie
nombre de demandes d'ouverture de session (SYN) en entrée et en sortie
nombre de hits sur règles

Host to host / host to router

Délais de réponse au ping avec une taille moyenne de paquet.

Outils open source : Ethereal, MRTG

Quelques événements affectant le niveau 3

Ajout d'équipement à adresse fixe

Serveurs, imprimantes => document modèle d'affectation d'adresse.

Mise en place d'un nouveau site

Implique maj du schéma global du WAN
Implique l'affection d'une adresse de réseau => document plan d'adressage.
Implique création d'un scope DHCP
Affection adresses : routeur, serveurs, imprimantes => document modèle d'affectation d'adresse.
Implique création des baseline pour le site

Panne de lien principal / backup

Arbre de décision + documentation lien backup ? Monté automatiquement ?
Pour se rendre compte de la panne d'un lien backup, il y a lieu de prévoir des 'exercices' périodiquement où on débranche la LS pour vérifier le bon fonctionnement (ou non) du backup (calendrier annuel)

Panne de routeur

Il est évident qu'on voudra redonder les routeurs critiques.
Le protocole CISCO est HSRP (Hot Stand By Router Protocol)
Si on est dans ce cas, il faut aussi tester le bon fonctionnement périodiquement (calendrier annuel)

Administration du niveau Infra-business Structure

Pascal Rodmacq - Juin 2006

Niveau 4 : services réseaux fondamentaux

Objets Physiques	Objets Logiques	Concepts	Information administrée
Serveurs Infrastructure	DHCP DNS NTP NDS AD LDAP SLP NDPS ZenWorks SMS SMTP POP IMAP SIP SNMP	Gestion de noms Authentification Représentation des objets du réseau Messagerie	Noms serveurs Adresses fixes Source de temps Conventions de nommage Arborescence

On ne conçoit pas un réseau TCP sans les services DHCP et DNS, ils constituent les services basiques minimaux de cet environnement.
Un réseau moderne doit distribuer une source de temps fiable : NTP
Ces services doivent être, par design, redondant, et doivent être surveillés.
Le messagerie est devenu un service vedette de toute entreprise dont le business ne saurait plus se passer.
L'annuaire doit être aussi un service non stop sur lequel repose l'authentification donc tout accès aux applications d'entreprise et même à son poste de travail.

Documentation grands services - 1

Il est intéressant de disposer les serveurs sur un schéma global du WAN. Ce qui permet de les situer et de mettre en évidence les flux.

DHCP

Liste des serveurs
Nom, adresse, OS, liste des scopes supportés
Par scope : les informations délivrées
Dynamic DNS ?

DNS

Schéma de l'espace de nommage
Schéma des serveurs et leur relation
Relation avec DNS internet
Liste des serveurs DNS
Nom, adresse, OS, version, Rôle, liste des zones supportées
Comportement des serveurs (récursivité, re-directeurs …)
Comportement des clients (requêteurs)

NTP

Représenter le schéma logique de distribution du temps avec les noms, adresse IP des serveurs (ou routeurs) concernés. Identifier la source de temps de référence.

Documentation grands services - 2

Annuaire

Arborescence logique.
AD : domaine, sous-domaine, OU, identification des contrôleurs de domaines (nom, adresse IP), maîtres opérateurs, catalogue.
eDirectory : arborescence des objets containers, limite de partitionnement, localisation logique des serveurs (nom, adresses), services supportés, repliquas supportés.

Messagerie

Nom, adresse IP, localisation des serveurs de messagerie avec leurs services, protocoles supportés.
Il y de plus en plus de services distribués associés à la messagerie (POP3, IMAP, Gateways, WebAccess … et de particularité suivant les éditeurs.
arborescence de certification et réplication pour Domino, notion de domaine, de post office, …

Inventaire des serveurs

Model / version de firmware / OS / interfaces / accès / affectation (site)
Id contrat de maintenance

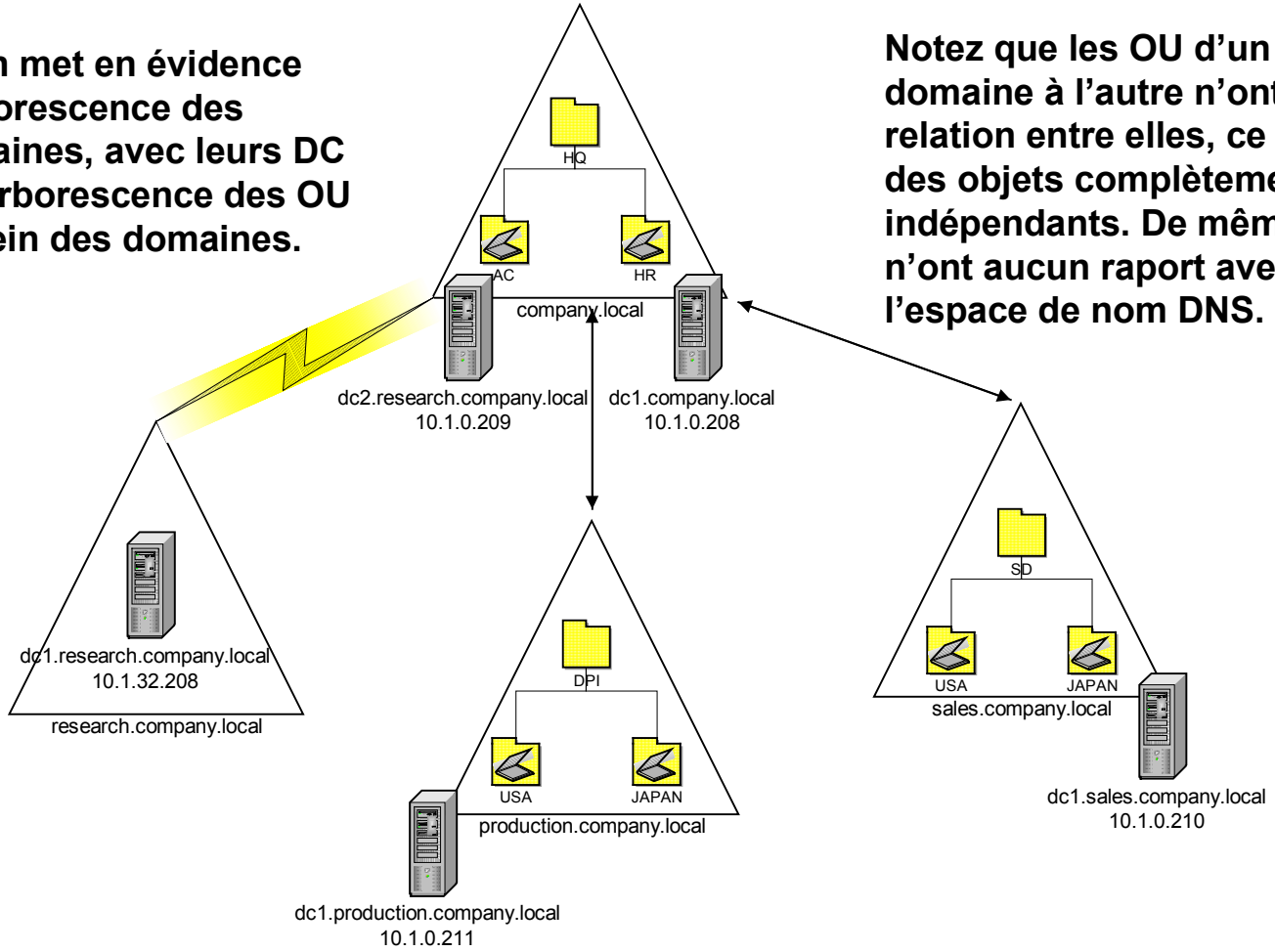
Exemple de schéma messagerie

C'est en créant ce schéma qu'il a été mis en évidence que le flux de messagerie interne à l'entreprise, entre 2 sites passait à travers le firewall. A la mise en place du firewall, le fournisseur avait créé les règles nécessaires pour laisser passer le trafic, ça n'avait paru étrange à personne, en fait l'information n'était jamais montée bien haut !
La technique, c'est si vulgaire !

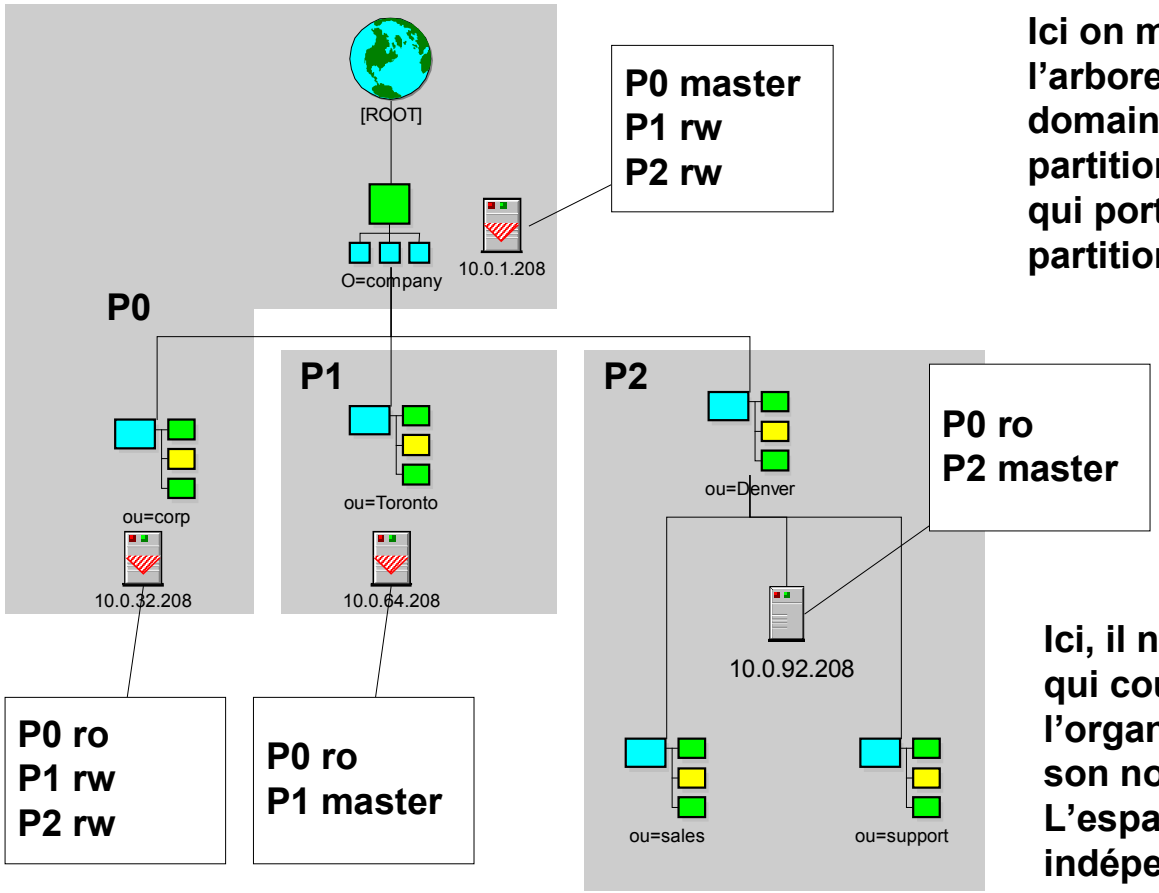
Exemple de schéma : Active directory

Ici on met en évidence l'arborescence des domaines, avec leurs DC et l'arborescence des OU au sein des domaines.

Notez que les OU d'un domaine à l'autre n'ont aucune relation entre elles, ce sont des objets complètement indépendants. De même ils n'ont aucun raport avec l'espace de nom DNS.



Exemple de schéma : eDirectory



Ici on met en évidence l'arborescence logique en domaine/sous-domaine, le partitionnement et les machines qui portent les réplicas des partitions.

Ici, il n'y a qu'une arborescence qui couvre l'ensemble de l'organisation. Chaque objet tire son nom de sa place dans l'arbre. L'espace de nom DNS est indépendant de cet espace de nommage.

Réplication et continuité de service

Pour l'essentiel, les grands services de bases sont conçus pour pouvoir assurer une continuité de service par design.
Le principe de fond de cette continuité est d'assurer la pérennité des données par réplication et de permettre aux clients de ces services d'utiliser indifféremment l'un ou l'autre serveur supportant une réplique.
Pour être efficace, ce système demande tout de même à ce qu'on s'intéresse au design, c'est le placement astucieux des répliquas sur des serveurs choisis qui garantit l'efficacité.
DNS a été d'emblée conçu avec un système de réplication, d'abord sur la mode Master/slave, (Multi master aujourd'hui avec Bind 9).
Parmi les pionniers, on compte Lotus dont l'offre Domino est fondé sur un système de réplication de base de données multi master très éprouvé.
Depuis longtemps les systèmes de messagerie ont offert un service de consolidation/réplication de carnet d'adresses global.
Aujourd'hui les annuaires sont les rois de la réplication, et les autres services commencent à leur sous-traiter les tâches de réplication qu'ils assuraient autrefois de façon autonome : c'est le cas d'Exchange 2000/2003 et de GroupWise 6 qui stockent leur configuration, et objets dans l'annuaire.
Notons quand même que les bases de messages pour Exchange et GroupWise ne sont pas répliquées, seules les configurations sont stockées dans un annuaire. (à la différence de Domino).

Réplication et continuité de service

En ce qui concerne DHCP et DNS Novell a une offre intégrée à Netware qui utilise l'annuaire comme stockage, et Microsoft a intégré DNS à Active Directory, pour ces 2 DNS, il n'y a plus de notion de réplication à gérer.

Toutefois, il ne faut pas oublier que si la réplication permet de se prémunir contre un désastre touchant une machine, elle ne prémunit nullement contre l'erreur (suppression malheureuse par exemple) qui elle va se répliquer !
Il faut donc quand même pouvoir se ménager des solutions pour pouvoir revenir à une situation antérieure saine.

Or les sauvegardes/restaurations de bases réparties répliquées posent des problèmes tout à fait différents de ceux des fichiers. Il y a plusieurs façons de sauvegarder qui impliqueront plusieurs façons de restaurer. (niveau base, niveau objet par exemple).
Un backup total niveau base est plus conçu dans l'optique de se protéger d'un sinistre total, assez peu probable, que d'une erreur ponctuelle.

Exemple de problématique :

Mon annuaire est corrompu, je peux encore ajouter et modifier certains objets mais je ne peux plus faire de suppression, la dernière suppression date de la semaine dernière. J'ai des sauvegardes journalières.
Que suis-je susceptible de perdre si je restaure ?

Annuaires : Surveillance Précautions

S’assurer du bon fonctionnement de la synchro horaire.

Vérifier les logs, notamment le processus de réplication.

En cas d’erreurs, chercher des explications, ne laissez pas pourrir la situation

Vérifier le statut des répliquas (sync, en cours, out of sync ?)

S’assurer qu’on a bien une redondance suffisante en terme de répliquas ou contrôleurs de domaines, notamment au cours de pannes, d’arrêts de machines, de mise à jours, etc … Il faudra penser à planifier ses arrêts de serveurs en fonction de leur rôle vis-à-vis de l’annuaire.

Limiter l’accès aux outils de réparation, écriture directe … qui peuvent être très dangereux et corrompre définitivement un annuaire.

Ne faites pas de modification significative sur votre annuaire sans vous êtes assuré de sa bonne santé auparavant.

La réplication à travers les liens WAN peut être assez lourde, des paquets perdus (CIR dépassé par exemple) sur le WAN peuvent perturber le processus de réplication.

Les 2 grands ennemis héréditaires de la réplication : liens WAN et synchro horaire ont perdu beaucoup de terrain depuis quelques années.

L’architecture SIP : principes

Les services de téléphonie sur IP ne sont pas encore dans la catégorie des grands services de bases comme DHCP DNS, toutefois, il est utile de prendre un peu les devants pour se rendre compte de ce qui se cache derrière et ce à quoi peut s’attendre l’administration, car on ne voit pas ce qui pourrait empêcher la voix de transiter majoritairement sur les réseaux numériques à moyen terme.

En fait, derrière la technicité des CODECS et de la QoS se cache une architecture qui fera largement appel à la résolution de noms et aux technologies d’annuaires.

La téléphonie classique est fondée sur des équipements (un équipement = un numéro), si vous avez 3 équipements, vous avez 3 adresses. SIP permet de basculer vers un modèle centré sur la personne, avec une adresse unique.

En interrogeant cette adresse, on localise la personne, sa disponibilité et les moyens qu’elle nous permet d’utiliser pour entrer en communication avec elle (téléphone, IM, messagerie …)

SIP, Session Initiation Protocol est décrit dans la RFC 3261.

Comme son nom l’indique SIP sert à ouvrir des sessions entre 2 partenaires. (et pas seulement des sessions VoIP en fait)

L'architecture SIP : les briques de base

AOR - Address of Record

Identifiant unique d'une personne.
SIP:pascal@rodmacq.com

URI - Uniform Resouce Identifier

SIP:0383353933@rodmacq.com;user=phone
SIP:0383353934@rodmacq.com;user=fax

UA - User Agent

l'UA est un programme dit UAC lorsqu'il émet une requête et UAS lorsqu'il répond à une requête (Client / Serveur) et B2BUA lorsqu'il fait les 2 simultanément. En tant que UAC, il initie une requête SIP, en tant que UAS, il transmet à l'utilisateur une requête SIP reçue et répond en fonction des décisions de l'utilisateur. On trouvera un UA dans un téléphone SIP, un softphone, un répondeur SIP, …

SIP Proxy Server

Intermédiaire qui reçoit des requêtes SIP et les route vers un autre proxy SIP ou un UA. Le proxy server se renseigne auprès d'un annuaire à propos du destinataire (par des requêtes LDAP ou SLP par exemple)

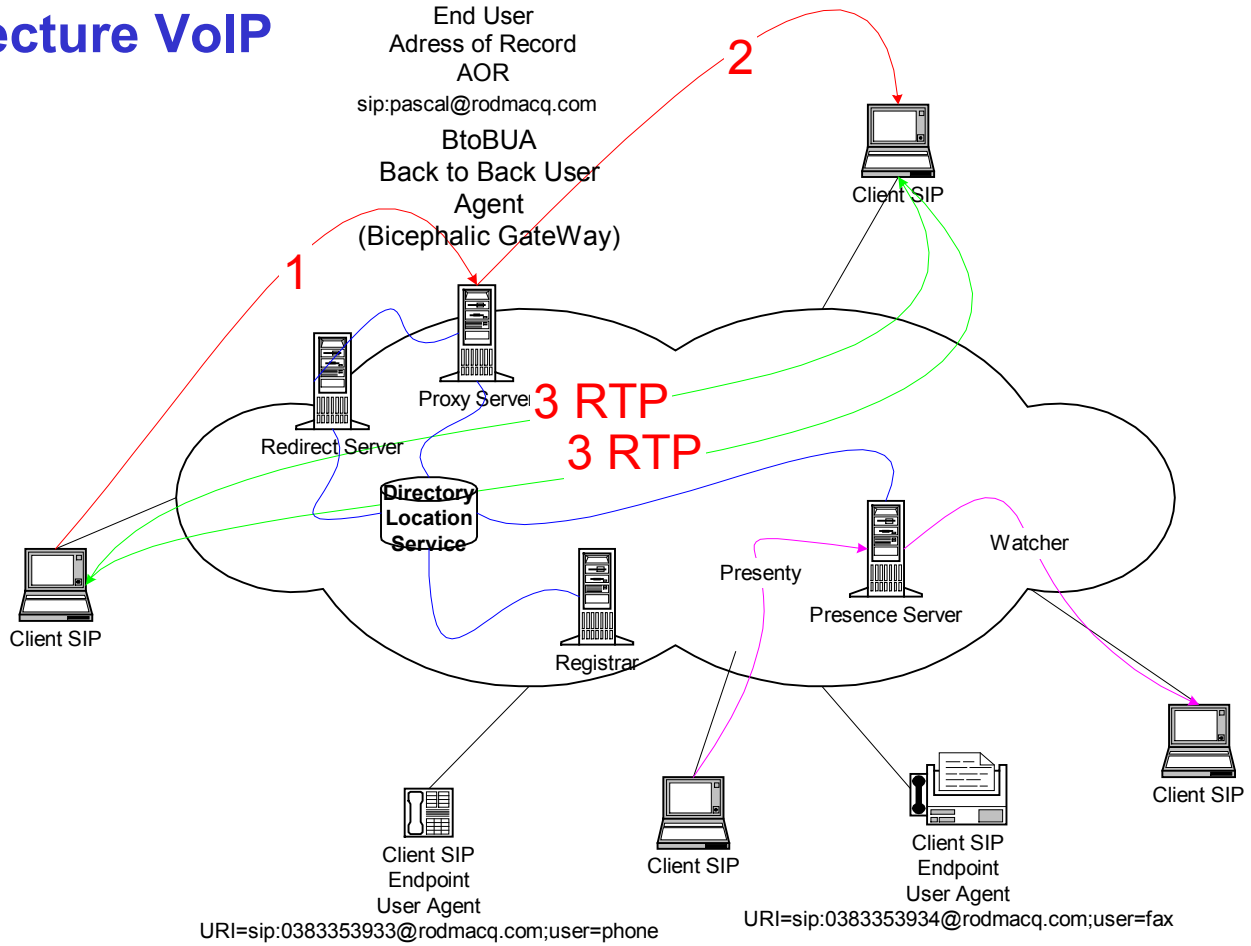
Redirect Server

Traite une requête SIP en répondant par une autre adresse (si possible) pour une adresse reçue : ce qui permet de rediriger un appel. Le redirect server prend typiquement ses renseignements dans un annuaire avec des requêtes LDAP.

Registrar Server

Traite les requêtes REGISTER des UA (ou d'un proxy) et met à jour une BdD les informations de contact de l'utilisateur (Typiquement le registrar va faire des requêtes LDAP vers un annuaire)

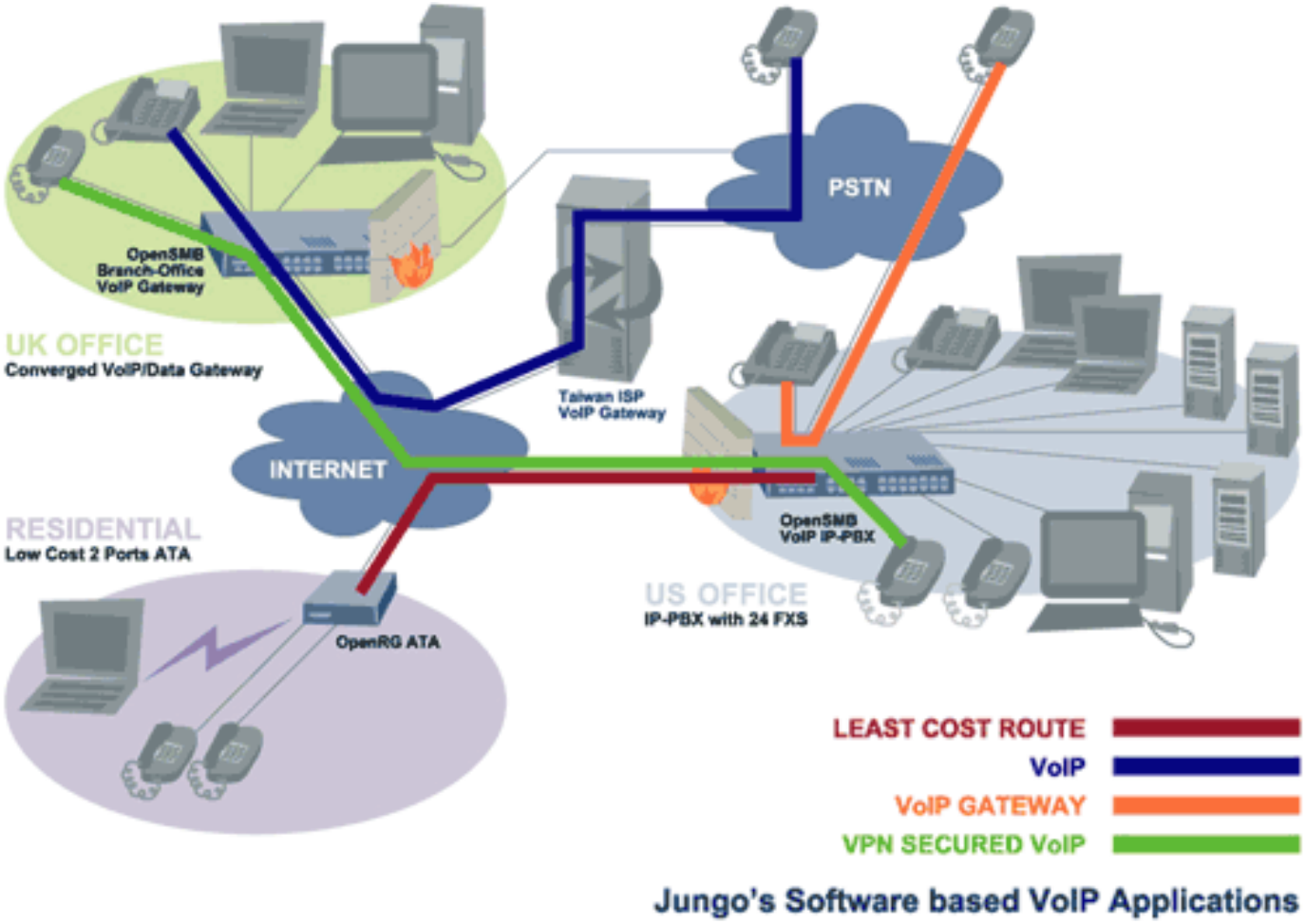
Les briques de l'architecture VoIP



UA = communication device
UAC = User Agent Client
(when requesting)
UAS = User Agent Server
(when requested)

Losqu'une device démarre, elle s'enregistre dans un Registrar Server ce aui permettra de renseigner les proxy server sur sa disponibilité.

Exemple d'offre actuelle



Les serveurs

Les serveurs restent les objets physiques les plus tangibles auxquels ait affaire l'administration au niveau 4.
Compte tenu de la criticité du support des grands services, il est logique de chercher à assurer leur continuité malgré la panne d'un serveur, le clustering est un moyen envisageable, que nous allons détailler plus loin.
Ce qu'on appelle serveur n'offre que peu de différence au fond avec n'importe quel poste de travail de la même génération.
Le packaging est différent : il y a une boite sérieuse, c'est rackable, on peut redonder l'alimentation, insérer un maximum de barettes mémoire, insérer plusieurs processeurs, plusieurs cartes réseaux, un ou plusieurs contrôleurs SCSI. Ces machines sont censées être livrées avec des drivers constructeurs « optimisés » pour les différents OS supportés.

En matière de serveurs, le modèle silo est en recul, là où il y a quelques années on avait typiquement un rack de serveurs indépendants avec chacun ses unités de stockages, on trouve maintenant de plus en plus de cluster de machine et un réseau SAN virtualise les unités de stockage pour un ensemble de serveur.
Nous allons dans un premier temps considérer les notions techniques de clustering et de virtualisation du stockage avant d'envisager les implications en terme d'administration (répartition de charge, haute disponibilité notamment, contraintes, charge d'administration)

Cluster - Définition

Un cluster peut être défini comme un ensemble limité (annoncé jusqu'à 32 - une dizaine typiquement) de systèmes interconnectés qui partagent des ressources de façon transparente.

Chaque sous-système – appelé nœud – est une machine complète avec processeur, mémoire, I/O et qui tourne sa propre instance d'OS.
Les clusters sont des ensembles dit faiblement couplés en ce sens que les processeurs ne partagent pas de mémoire comme les systèmes à multiprocesseurs symétriques.

Le concept a été introduit par TANDEM à la fin des années 70. Sur le même schéma DEC mettra VAXcluster sur le marché en 83.
TANDEM et DEC poursuivaient des objectifs totalement différents : TANDEM voulait fiabiliser ses systèmes transactionnels, DEC voulait booster la performance de ses VAX (arrivés en retard sur le marché).

Ces architectures se retrouvent totalement dans les clusters actuels sur UNIX (Linux), Microsoft, Novell 5 & 6 (SFT III totalement original mais arrêté), ces systèmes classiques n'utilisent pas de mémoire partagée à la différence de l'offre IBM Sysplex.

Cluster – mise en oeuvre

Le cluster se compose de machines homogènes avec le même OS (même release) adapté pour le clustering ou l'OS standard + un service cluster.
Vue de l'extérieur, le cluster donne l'impression d'être une seule machine.
Déjà, il y a une adresse réseau pour l'ensemble du cluster (ce qui n'empêche pas chaque machine d'avoir sa propre adresse).
Les ressources partagées par le cluster seront appelées ressources «clusterisées» et doivent être gérées en tant que telles.
Les serveurs seront généralement contiguës, dans la même pièce, constituant une unité de maintenance (on peut les répartir sur le réseau mais cela peut présenter des complications pour la maintenance)
La synchronisation entre les nœuds est gérée par ce qu'on appelle le DLM (de Distributed Lock Manager, hérité du jargon VAX)
L'OS peut être spécifique (Tandem) ou un OS adapté (Sysplex adapté de VMS, Unix clusterisé, MCCS l'adaptation de Windows, NetWare 6.5 est en standard clusterisable (limité à 2 nœuds commercialement)
En général, il y a un nœud maître et un échange de heartbeat pour une vérification mutuelle de l'activité des nœuds.
Si on veut clusteriser des applications qui utilisent des données (c'est souvent le cas), il faut aussi un espace de stockage commun aux nœuds du cluster. Ce volume logique ne doit pas être accédé par des machines hors cluster sous peine de corrompre l'organisation du volume.

Cluster : support des applications

Les machines du cluster possèdent donc en général une patte sur le LAN et une patte sur un réseau SAN.

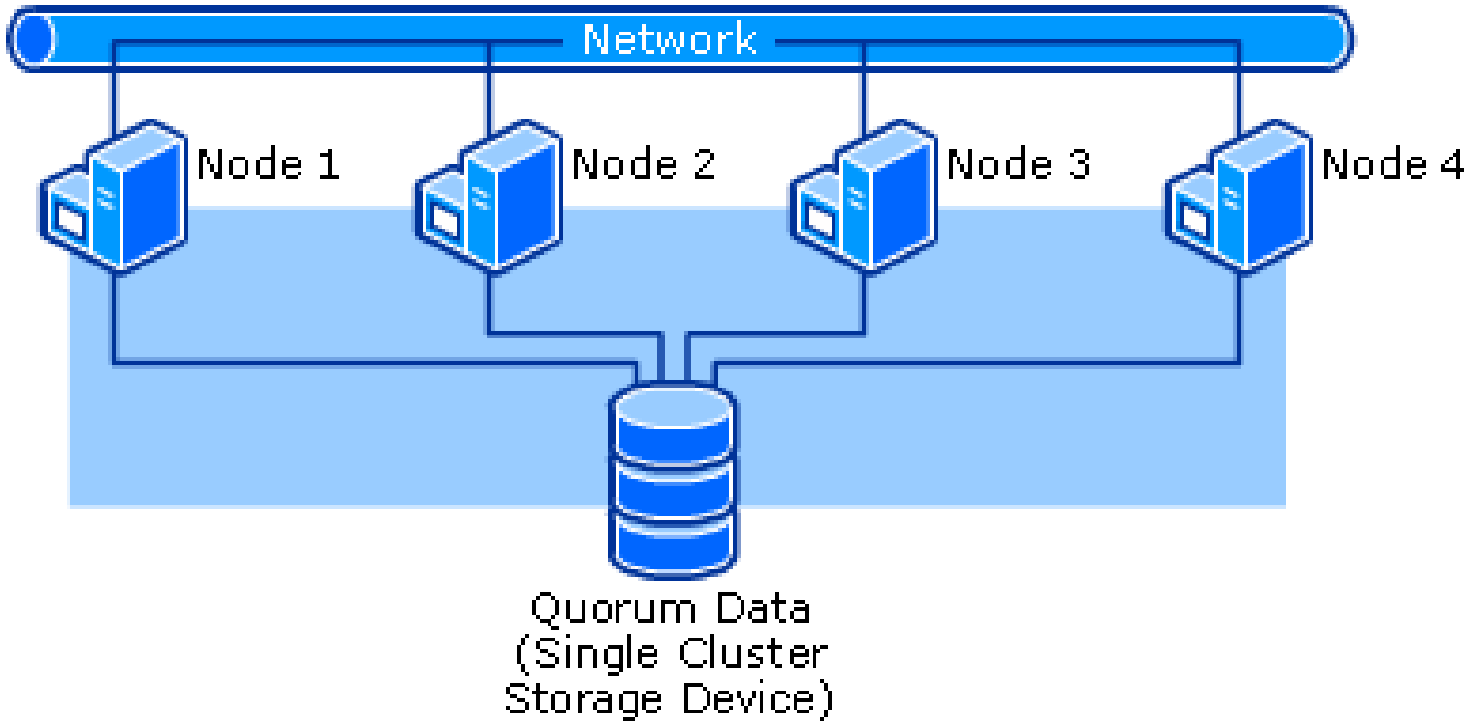
Nature des applications clusterisées :

Stateless : opérations courtes traitées indépendamment les unes des autres, sans avoir besoin de se souvenir d'un état précédent, ou ne faisant que de la lecture de données.
Exemples : serveur ftp en lecture seule, serveur web frontal, VPN server, firewall (ISA Server).
Ces applications peuvent tourner tel que, à la rigueur elles utilisent une petite zone de mémoire disque partagée dans lesquels elles enregistre un ID de transaction qui permet de suivre les états d'une transaction.

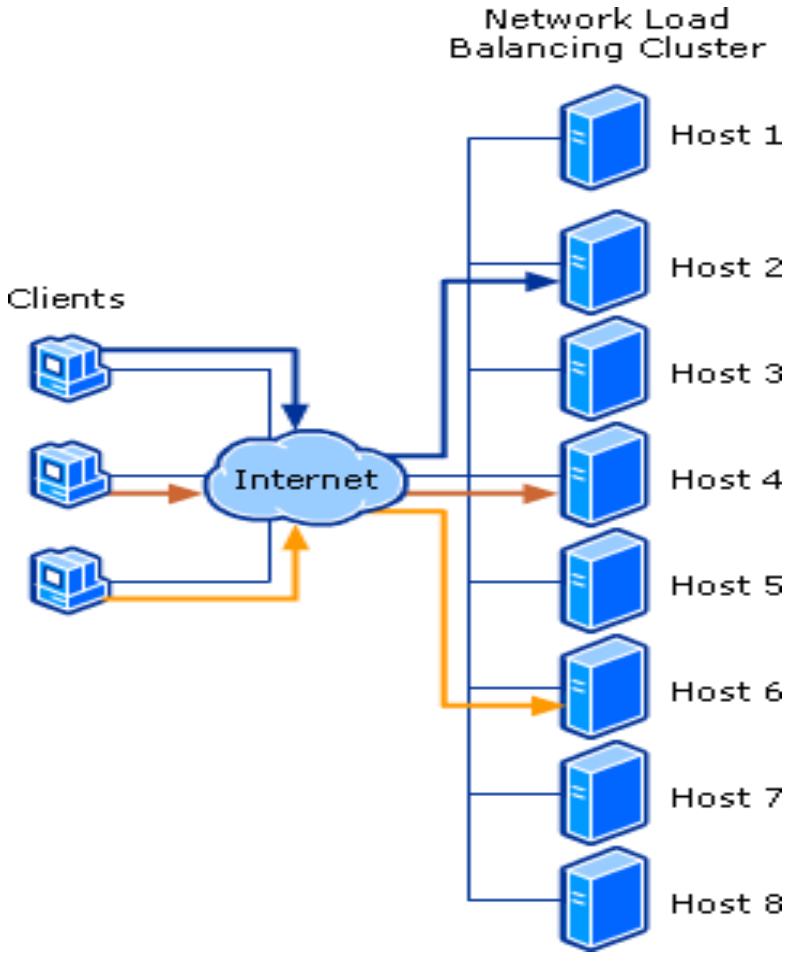
Statefull : les applications gèrent des transactions longues passant par des étapes successives, la réalisation d'une étape implique de se souvenir de la précédente, nombreuses opération d'écriture de données. Exemple : SGBD

Un cluster donné supportera en général un des modes exclusivement de l'autre. Cas du clustering Microsoft qui dans son jargon parle de load balancing pour le premier cas, et clustering pour le second et limite alors le nombre de nœuds à 8, les applications supportées sont SQL Server et Exchange (elles doivent être conçues pour cela)

Cluster sur SAN



Clustering type Load balancing



Cluster : maintenance

Derrière une apparente simplicité, les clusters peuvent cacher pas mal de complications au quotidien.
Déjà, il faut pouvoir identifier que des machines sont en cluster, il y a intérêt à les distinguer physiquement dans la salle machine, s'il y a plusieurs clusters, il faut étiqueter en conséquence.

Il y a des informations spécifiques à documenter :

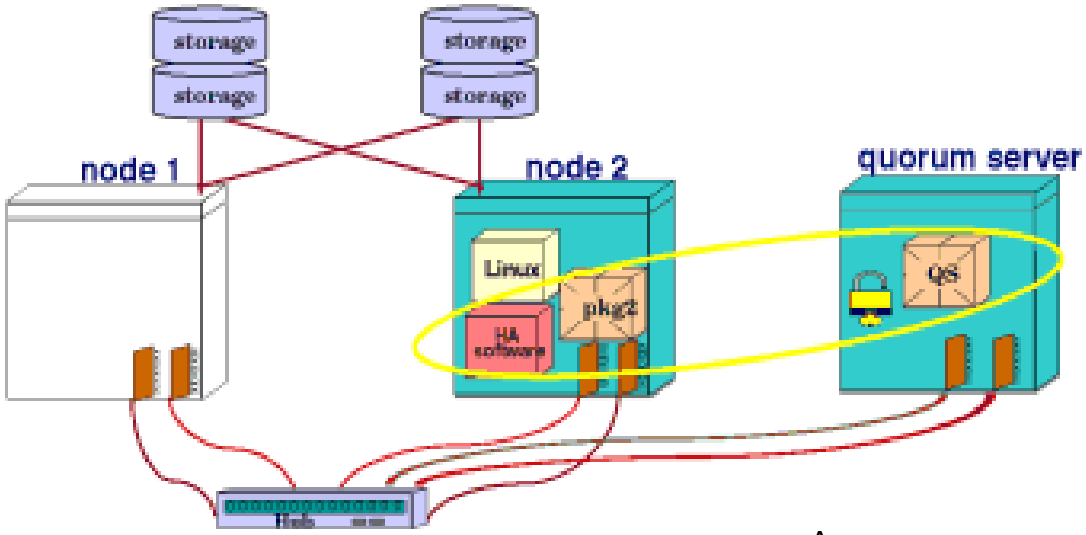
Nom du cluster
Liste des machines
Réglage du Hearbeat
Liste des applications clustérisées
Définir les décisions à prendre suivant des scénarios de défaillance (vers quel nœud faire redémarrer une application …)
Bref tout ce qui constituera le fichier de paramètres du cluster et qui devra être répliqué sur toutes les machines du cluster.

Il y a toute une panoplie de situations « amusantes » :

Le nœud s'endort, il est débranché du cluster par les autres. Il se reveille et pense qu'il est toujours membre du cluster …

Split brain : le cluster s'est coupé en 2 chaque partie pensant être unique …

Lutter contre le split brain …



Peut entraîner pas mal de complications …

Ci-dessus la notion de quorum serveur, contrôlant un cluster et imposant un choix lorsqu'un split est détecté.
(document Hewlett packard)

A quorum server can be used in clusters of any size. In a two-node cluster, you are required to configure the quorum server. If communications are lost between these two nodes, the node that obtains the cluster lock will take over the cluster and the other node will perform a TOC. Without a cluster lock, a failure of either node in the cluster will cause the other node, and therefore the cluster, to halt. Note also that if the quorum server is not available during an attempt to access it, the cluster will halt.

Cluster - conclusion

On a vu que, parmi les services de bases de l'infra-business structure, DNS et Annuaire étaient fault tolerant par design, de part la réplication des données et c'est également le design, forme de l'annuaire et disposition des serveurs et services qui permet de répartir la charge. Pour ces services, la clusterisation n'a rien à apporter, à part des complications.
DHCP peut l'être aussi de la même façon, mais l'offre est plus rare. (Novell est l'offre abordable, il y a des offres spécialisées fault tolerant mais très coûteuses), enfin DHCP est facile à protéger dès lors qu'on dispose d'assez d'adresses par la technique du scope dormant sur un serveur tiers.
Pour la messagerie, le problème est bien aussi de protéger les données. Maintenant certaines fonctions de la messagerie peuvent être clusterisées : par exemple la réception de messages SMTP, en fait, c'est une forme de load balancing qui est alors pratiqué. (en l'absence de cluster, on pratique un round robin DNS par exemple, à la différence que dans ce dernier cas on ignore à priori la charge de la machine choisie).

Et en fait, d'une manière générale, on peut conclure que l'utilisation de cluster faiblement couplée est beaucoup plus destiné au load balancing qu'à n'importe quoi d'autre.

Ce ne peut pas être une solution généralisable pour se prémunir de la panne d'une machine en général, c'est un moyen à mettre en œuvre pour des services bien délimités pour lesquels on veut assurer tenue de charge et disponibilité.

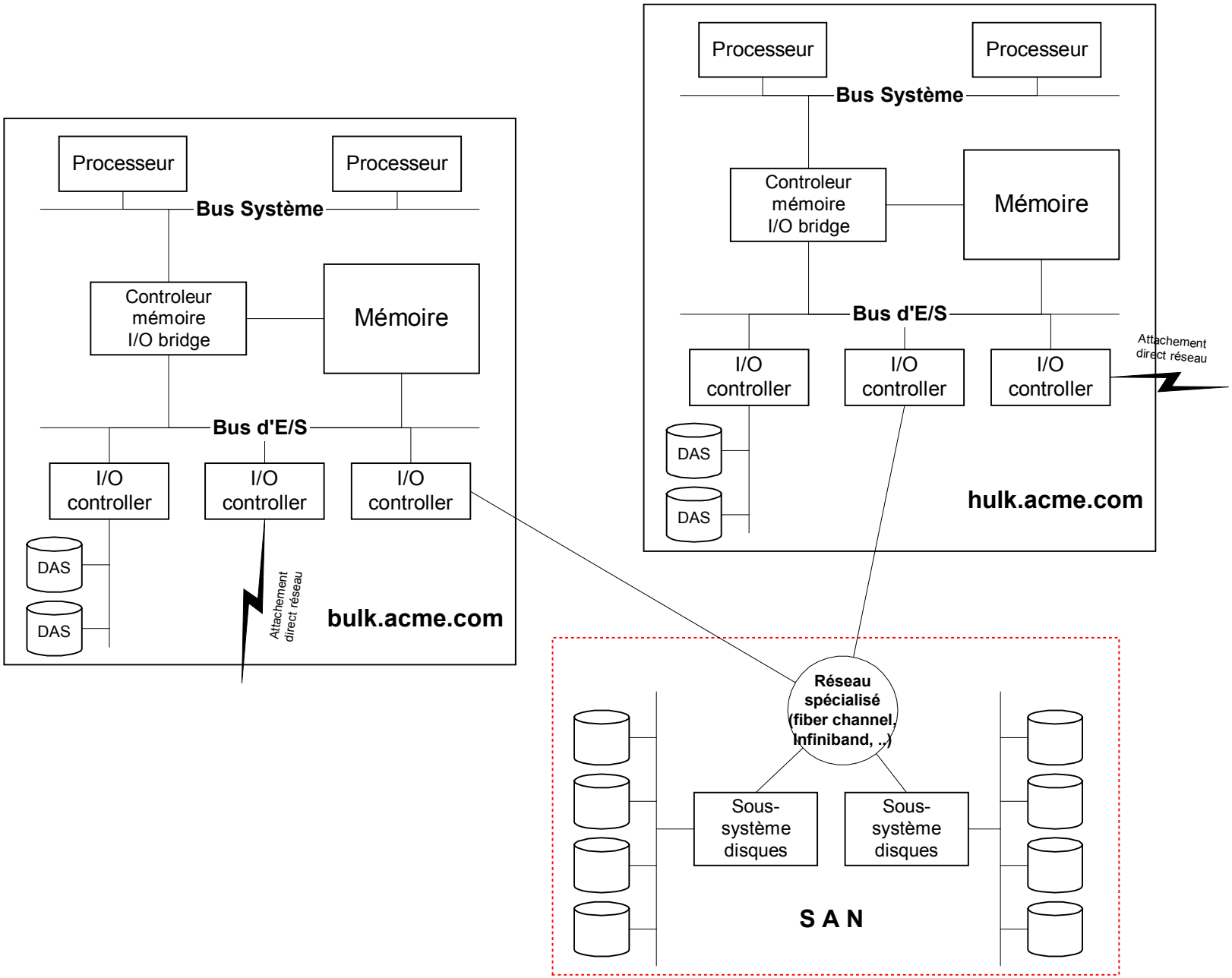
DAS, SAN, iSCSI, NAS and Cie …

L'explosion des données (nous analyserons ce phénomène d'un peu plus près) au sein de l'entreprise et l'émiettement des capacités de stockage sur les divers serveurs ont amené les problèmes suivants : limitation des systèmes de stockage classiquement attachés au serveurs (une baie SCSI en RAID 5 avec une dizaine de disques), la nécessité d'avoir à gérer de multiple points de sauvegarde, la désolation de voir des capacités inutilisées sur une machine alors qu'on doit étendre une baie de disque sur la machine voisine.
Ceci a amené un raisonnement mutualiste : mettons tous les disques dans le même panier et donnons nous les moyens de pouvoir piocher la capacité nécessaire et de l'affecter au besoin à telle ou telle unité logique au niveau de l'OS.
Bref, découpler la fonction de stockage de l'OS pour la confier à un élément spécialisé.

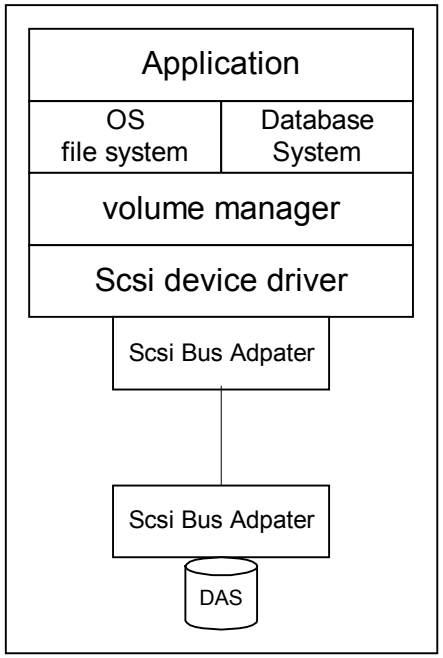
Cette idée a trouvé son chemin à travers le bus SCSI, dont la norme définit un protocole de communication entre un contrôleur et une device SCSI. Ceci est le principe fondateur, à partir du moment où on a un protocole, on peut découpler physiquement les systèmes qui communiqueront à travers ce protocole. Cette idée est la base du SAN et de iSCSI. On empaquette des requêtes au niveau blocs d'E/S qu'on transmet aux devices sur un réseau spécialisé. La machine cliente reste maîtresse de ses volumes.

Le NAS lui est très proche de la notion de serveur de fichier. Une couche logicielle trappe les appels au système de fichier émis par la machine cliente dans son jargon (NFS, CIFS …) les empaquette et les transmet à un autre système chargé de traiter la requête avec son propre file system. Dans ce système, la gestion des volumes est déportée vers le serveur, ce qui permet la virtualisation. La machine cliente « monte » un volume virtuel puis travaille dessus à la façon habituelle.

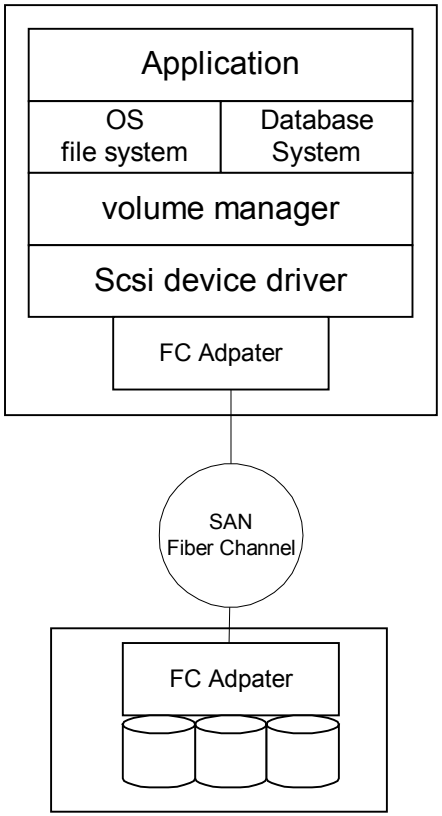
S A N


Processeur
Processeur
Bus Système
Controleur mémoire I/O bridge
Mémoire
Bus d'E/S
I/O controller
I/O controller
I/O controller
DAS
DAS
Attachement direct réseau
bulk.acme.com
Processeur
Processeur
Bus Système
Controleur mémoire I/O bridge
Mémoire
Bus d'E/S
I/O controller
I/O controller
I/O controller
Attachement direct réseau
DAS
DAS
hulk.acme.com
Réseau spécialisé (fiber channel, Infiniband, ..)
Sous-système disques
Sous-système disques
S A N

Architecture DAS SAN iSCSI

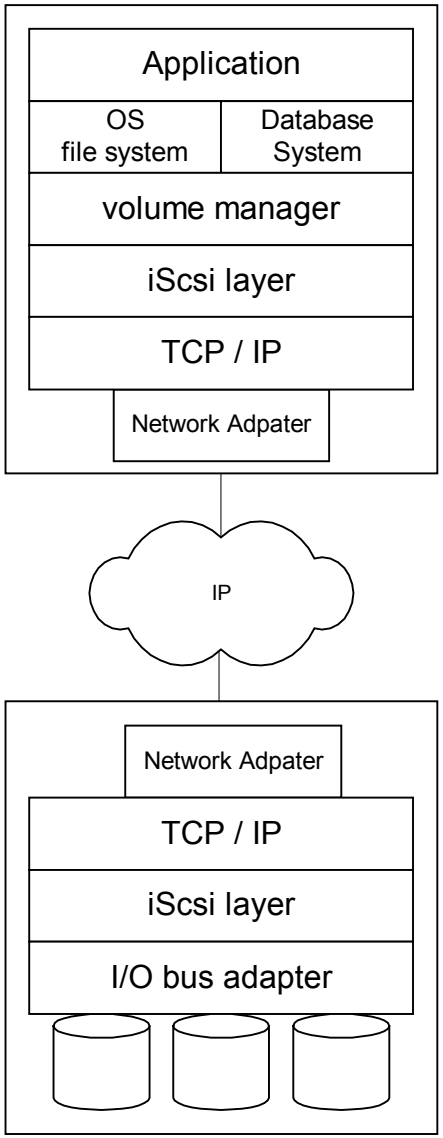


DAS

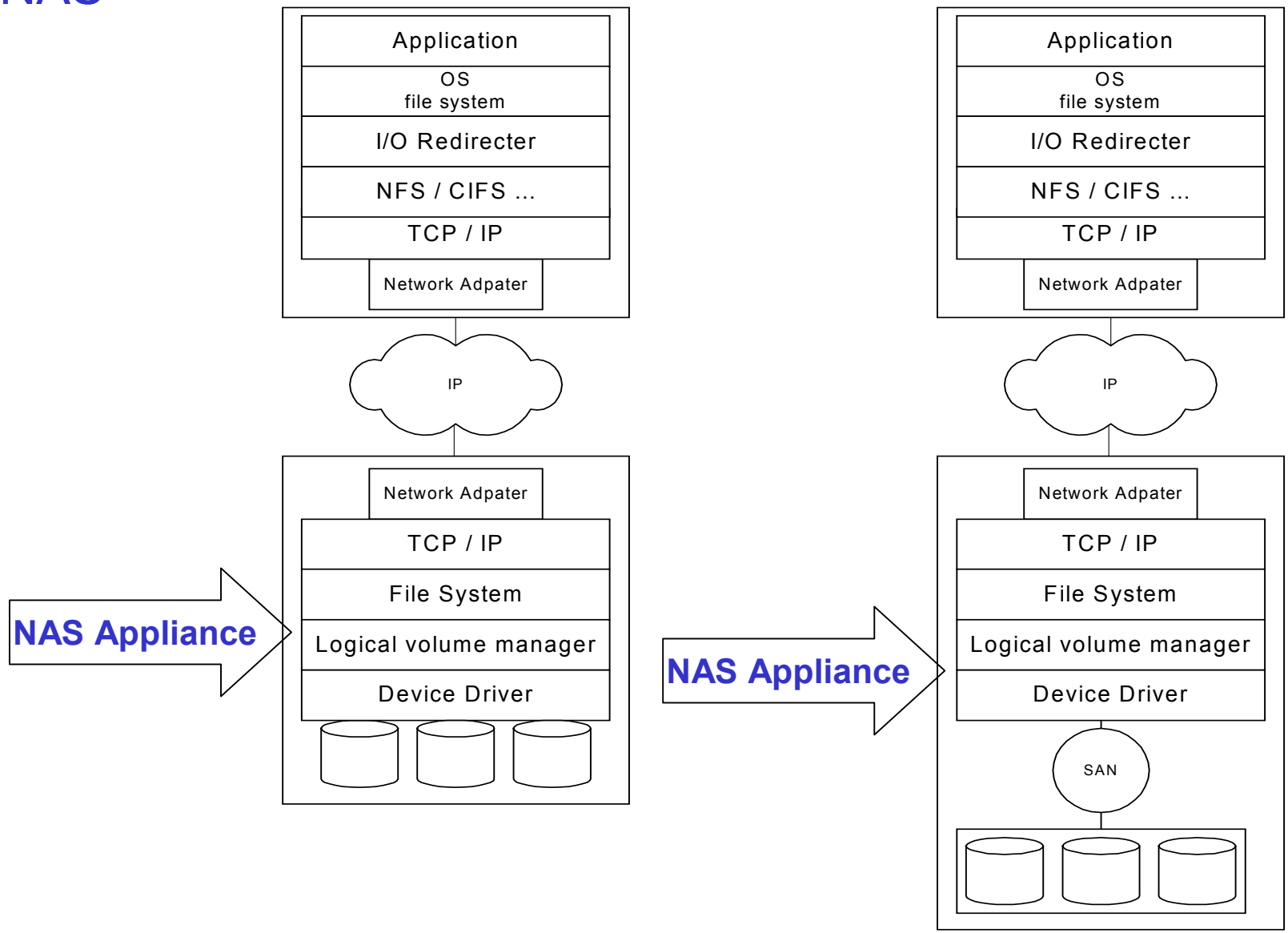


SAN

iSCSI



NAS


Application
OS
file system
I/O Redirecter
NFS / CIFS ...
TCP / IP
Network Adpater
IP
Network Adpater
TCP / IP
File System
Logical volume manager
Device Driver
NAS Appliance
Application
OS
file system
I/O Redirecter
NFS / CIFS ...
TCP / IP
Network Adpater
IP
Network Adpater
TCP / IP
File System
Logical volume manager
Device Driver
SAN
NAS Appliance

SAN / NAS : une offre encore brouillonne

Le beurre et l'argent du beurre

SAN / iSCSI permettent une centralisation des données, et par le découplage du stockage le partage de l'investissement associé, et un investissement à priori plus incrémental. Notons aussi que cet argument perd du poids avec la diminution du coût des disques.

Les sauvegardes, peuvent être grandement améliorées, elles deviennent LAN free et Server free, cad qu'elles n'impliquent plus ni l'un ni l'autre, on peut se permettre des sauvegardes continues, snap shots …

Leur inconvénient majeur et que, les différentes machines restent maîtresse des volumes et qu'une fois un volume allouée à l'une, son espace n'est pas allouable à une autre sans une véritable ingénierie, donc l'idée d'investissement incrémental peut être limité ici.

Pour pallier à cela, on introduit le NAS et un élément purement logiciel (un véritable OS en fait) qui permet d'offrir une vue habituelle au système de fichier des clients tout en faisant sa sauce avec les disques, il n'y a alors, physiquement qu'un espace, donc plus de disputes !

L'inconvénient est que le schéma est plus complexe (en fonctionnement, pas en installation), plus lent certainement et plus complexe ensuite en administration car il introduit un niveau d'administration supplémentaire.

Management SAN / NAS : attention à la complexité

Le sous système de disques est livré avec un outil de management, le switch Fibre Channel est livré avec un outil de management. La gestion du serveur SAN se fait à travers un outil de management. Bref trois outils de management parallèles qui multiplient la charge par 3 puissance 2 (Pascal's Law : La charge de Management évolue comme le carré du nombre de plate formes de management).

Aujourd'hui, le marché est rempli d'une offre SAN pléthorique, avec des offreurs proposant des solutions propriétaires ou partiellement propriétaires. Ceci signifie que ces produits ne fonctionnent pas toujours ensemble, ou du moins fonctionnent avec des restrictions au niveau de chaque sous composant.

Administration du niveau Business Structure

Pascal Rodmacq - Juin 2006

Niveau 5 : niveau application environnement utilisateur

	Objets Physiques	Objets Logiques	Concepts	Niveau
5	**Postes de travail Serveurs de fichiers et applications**	**OS Stations Données Applications**	**Environnement utilisateur / Service**	**Business Structure**

Sans doute le niveau le plus difficile pour l'administration SI, le point de contact avec les clients, les données, la sécurité.

Les thèmes vedettes de ce niveau seront les données et les applications.

Data : déluge et désordre !

« The University of California, Berkeley, just released a study predicting (threatening?) that more data will be created in the next three years than was created in the last 40,000 years » Janvier 2006

Gartner Group prétend qu'il en coûte 5 à sept fois plus cher pour manager le stockage que pour l'acheter ! Simultanément, le prix par MB chute alors que les coûts liés à la sécurité, fiabilité, et management sautent au plafond.

Notons le cercle vicieux : plus le Ko est bon marché, plus on a tendance à en acheter et plus il nous en coûtera cher en administration !

En fait la technologie des disques dans un poste de travail et dans un serveur de fichier est la même, et ce qui se passe c'est que, très vite, la taille des disques sur les postes de travail dépasse celle des disques sur les systèmes de stockage, qui se renouvellent moins vite que les stations, or il y a des milliers de stations de travail …

Les données des utilisateurs se nichent dans les refuges suivants :

-le système de fichiers : sur serveur et/ou sur poste de travail individuel (le plus souvent les 2 de façon indistincte et non gérée avec la rigueur nécessaire)
- la messagerie : dans la boite individuelle de l'utilisateur qui a tendance à grossir sur une courbe ne montrant aucun signe d'inflexion.
- les données gérées par des applications, le plus souvent dans des bases de données, aujourd'hui, ces dernières représentent, de loin le volume le plus faible !
- il y a aussi des données publiées sur des dossiers partagés de messagerie (groupware) et sur les services web de l'intranet.

Data : déluge et désordre !

En fait, historiquement (encore) les données n'existaient qu'à travers des applications, elles étaient nécessairement structurées et leur créeation / maj sous contrôle. Les utilisateurs n'avaient pas accès au système de fichier directement.

L'accès direct au système de fichiers de l'OS s'est fait avec l'introduction des micro-ordinateurs et tant que les disques sont restés à taille humaine, les utilisateurs étaient à peu près capables d'en gérer le contenu avec un explorateur. Ce qui n'est plus du tout le cas aujourd'hui.

Avec les serveurs de fichiers sur le LAN, on a assisté à un mouvement de structuration : définition d'une arborescence de données commune à l'entreprise avec un système de permissions. Mais ce mouvement ne s'est pas imposé, cette démarche est rarement prise au sérieux dans les entreprises, on n'y voit pas l'intérêt.

On constate que, moins l'information est structurée, plus elle occupe de volume, en fait ce qui se passe à un certain moment c'est qu'essentiellement on n'est plus capable de supprimer : la durée de moyenne d'une information tend vers l'infini ! On ne sait plus distinguer une information morte, on ne sait plus quelle est la bonne version … dans le doute, on garde tout.

Data : organiser, hiérarchiser, gérer le cycle de vie !

Moyens de lutte au niveau du système de fichiers :

- Etablir des quotas sur les répertoires individuels.

- Bannir le répertoire public fourre-tout rempli de tout et n'importe quoi.

- Prodiguer un cadre efficace : arborescence claire, justifiée, publique, documentée, mise à jour, procédures de demande/maj de droits connues, simples et rapides sous le contrôle du business.

- Définir des périmètres de donnée avec un niveau de criticité et de confidentialité, avec un responsable (business) pour l'attribution des droits, l'évolution du design, la politique de sauvegarde.

- Distinguer les notion de données actives / archives, les dossiers devraient toujours comporter des sous-dossiers d'archives.

- Avoir une procédure de déclassement : au delà d'un temps donné, les archives doivent sortir définitivement du disque pour être supprimées ou passer sur support externe en fonction de décision business.

- Envisager la hiérarchisation des données en fonction de la fréquence d'accès, cette technique n'est pas en vogue sur le marché actuellement pourtant c'est peut être ce dont on aurait le plus besoin.

- Bref : implanter un système de gestion du cycle de vie de l'information !

Data : dominer l'information

- Maintenant, il faut aussi considérer que l'utilisation du seul gestionnaire de fichiers dans sa plus simple expression devient vite insuffisante pour gérer et retrouver des milliers de fichiers, il faut éduquer les utilisateurs à normaliser les noms de fichiers et à faire des recherches sur les noms, les dates et éventuellement le contenu.

- Utiliser des outils d'organisation des données du type knowledge organiser (MindManager, MindGenius, FreeMind … développés d'après le concept de « mind mapping » du psychologue anglais Tony Burzan) peut aussi aider à dominer la prolifération des datas en élevant le niveau de contrôle sur la création et l'organisation des datas.

- On peut espérer voir naître d'autres outils et peut être que l'accès aux données via le gestionnaire de fichiers

- En attendant, on voit se développer en ce moment la solution qu'on pourrait appeler de type « force brute » : NAS / SAN à tout va. Notons que, alors que le prix des disques a considérablement chuté, le coûts des systèmes de stockage vient manger ce gain.

- Il est tout de même paradoxal de voir une grande partie de l'information utilisée par l'entreprise presque totalement livrée à elle même !

Data : analyser les flux

Moyens de lutte au niveau de la messagerie

Etablir des quotas sur les boites

Bien distinguer entre la fonction transport / acheminement des messages d'une part et la fonction stockage des données qui constitue en quelque sorte un deuxième niveau de gestionnaire de fichier dans un espace séparé. Beaucoup d'utilisateurs se retrouvent avec 2 espaces de gestion parallèles de leurs données : celui du gestionnaire de fichier et celui de la messagerie.

Eduquer les utilisateurs à détacher les pièces jointes, ou à utiliser d'autres moyens que la messagerie pour transférer des rapports à un groupe d'utilisateurs par exemple (le typique Excel de reporting de 150 Mo envoyé tous les mois à 10 destinataires devrait être déposé sur un répertoire partagé, éventuellement répliqué si les utilisateurs sont répartis à travers le WAN).

Ceci est typique : la bande passante n'est pas suffisante pour ouvrir le fichier Excel à travers le WAN, alors on l'envoie partout par la messagerie, créant ainsi une duplication des données qu'on ne sera plus capable de mettre à jour. Ultérieurement, la bande passante devient suffisante mais la pratique ne changera pas.

Evolution historique des architectures applicatives

- Les mouvements de fond qui animent l'évolution de l'architecture des SI ont une influence sur la structuration et le contenu des tâches d'administration.
- La connaissance de ces mouvements de fond permet d'anticiper les tendances et de comprendre où se dirige « naturellement » l'administration.

PS : il va de soi, que ce mouvement « naturel » n'est pas forcément à l'avantage de l'entreprise et qu'il n'y a aucune raison pour le subir sans réaction.

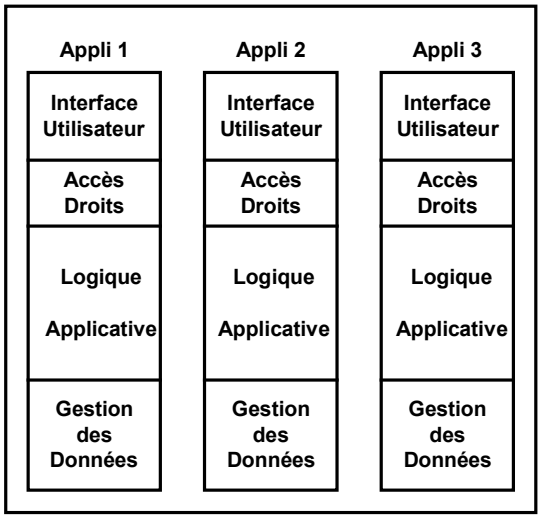
Evolution du modèle d'architecture applicative

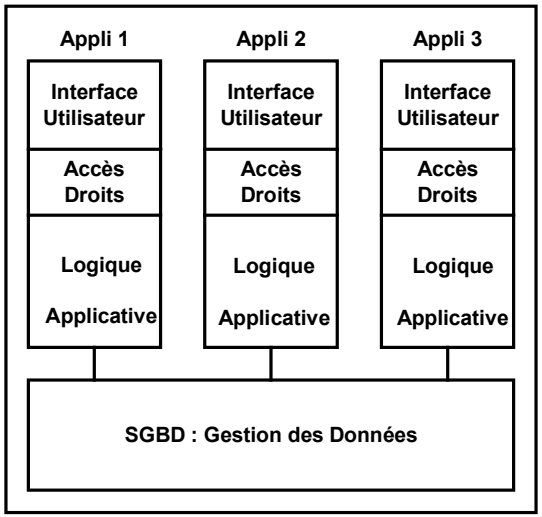
1 – le modèle SILO cède du terrain

Historiquement, les applications se sont développées dans les entreprises sur un modèle en silos. C'est-à-dire que chaque application intégrait tout : de l'interface utilisateur à la gestion des données en passant par la gestion des accès.

La première fonction à être sortie de ce modèle est celle de la gestion des données avec la mise en oeuvre des bases de données à la fin des années 70. La gestion des données sortaient de l'application pour être confiée à une couche spécialisée.

On a alors commencé à parler d'administrateur de Base de Données …

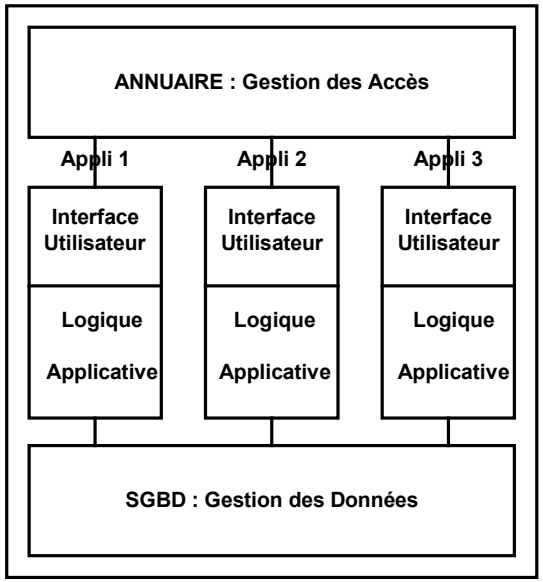




Evolution du modèle d'architecture applicative

2 – de plus en plus de terrain …

De la même façon, il y a maintenant un mouvement visant à sortir la gestion des droits et accès des applications pour confier ces tâches à un annuaire central, transverse.
On n'en pas tout à fait encore à demander des administrateurs d'annuaires, mais ça ne saurait tarder ! (c'est déjà sous-entendu lorsqu'on demande un administrateur Windows 2000 ou Novell)



Qu'attend-on de ce mouvement ?

Par la centralisation et l'adoption de méthodes uniformes pour l'ensemble des applications, on peut espérer :

- d'une part une normalisation, un allégement et une meilleure structuration des applications.

- d'autre part une meilleure vue sur la sécurité en regroupant l'ensemble des données concernant les droits et autorisations sous un système de gestion uniforme et en permettant une meilleure organisation par la séparation des tâches liées spécifiquement à la sécurité.

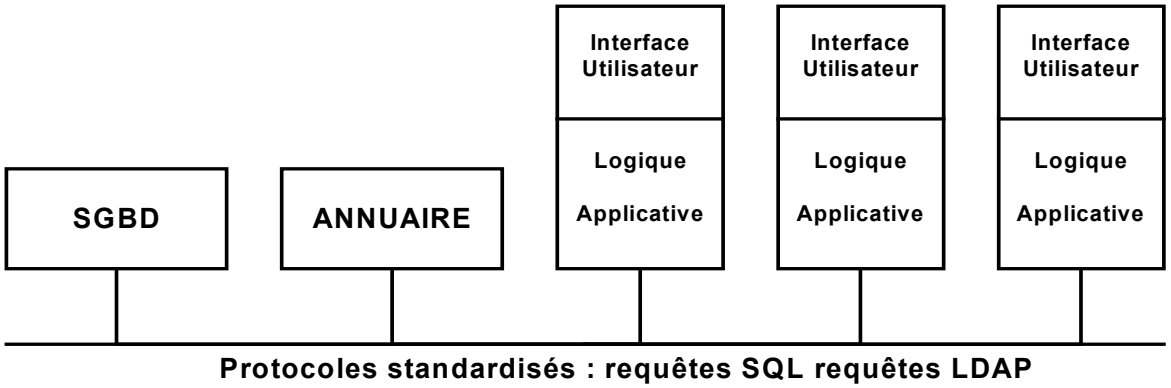
Evolution du modèle d'architecture applicative

3 – de plus en plus de terrain …

Avec l'introduction de la variable réseau, il faut prendre en compte d'autres problèmes : il faut pouvoir localiser les services sur le réseau, il faut un protocole de communication adapté, il faut pouvoir distribuer l'annuaire à travers les différents sites dans un contexte WAN. Ces derniers paramètres impliquent de considérer l'architecture du réseau au niveau transport et disponibilité des grands services de bases, notamment la résolution de noms.

Enfin, les données s'échangeant à travers un réseau, entre des process distincts, la sécurisation implique une réflexion différente de celle traditionnelle, fondée sur l'accès à une machine.

Les problématiques ci-dessus, de localisation des services et de sécurité (identification, intégrité, confidentialité) seront d'autant plus exacerbées que l'on voudra permettre l'accès des applications à des personnes extérieures à l'entreprises (clients, partenaires) non gérées comme des utilisateurs internes du système.



Conséquences pour la fonction d'administration

La multiplication des applications en silos a eu les effets suivant :

- **la nécessité de gérer des utilisateurs et permissions pour chaque application impliquant une charge d'administration multipliée.**
- **la nécessité pour les utilisateurs de retenir autant de mots de passe que d'applications utilisées posant une menace pour la sécurité. Nécessairement l'oublie ou la confusion entre tous ces mots de passe, ajoute une charge totalement improductive sur la fonction d'administration.**
- **la nécessité de mettre en place des interfaces entre les applications entraîne une charge d'exploitation et une rigidité induite par la complexité.**

L'apparition des bases de données a eu pour effet :

- **la nécessité de dominer un nouveau champ de compétence.**
- **la mise en place de techniques de sauvegarde de données spécifique en plus de celles existantes.**
- **certaines applications continuent l'effet silo en imposant une base de données spécifique ajoutant une charge de plus pour l'administration.**

L'apparition des annuaires a pour effet :

- **la nécessité de dominer de nouveaux champs de compétence en terme d'infrastructure, de design d'annuaire et de méthode d'administration des utilisateurs.**
- **encore une spécificité pour la sauvegarde des données de l'annuaire … et la plupart des applications en place ne savent pas tirer partie de l'annuaire**

Espoirs pour la fonction d'administration

Constat :

La mise en place des nouvelles technologies au sein des services ne s'est pas faite avec l'optique de diminuer la complexité ni d'améliorer la souplesse de l'organisation, les critères de choix n'ont - en général - pas intégré les nécessités de la fonction administration.

Utilisation des bases de données :

- Aurait dû permettre de séparer vraiment la gestion des applications de la gestion des données et de donner un accès uniforme aux données des applications à travers des outils standards. (en fait on n'est même plus d'accord sur SQL)
- Un seul système de base de données devrait être supporté et maintenu et toute application nouvelle devrait s'y plier, faute de quoi, elle perdrait toute chance d'être acheté => cet élément s'élève au rang de critère de sélection fondamental pour l'administration.
- Le SGBD sélectionné devrait l'être en fonction de son respect des standards, de sa portabilité, du découplage de sa facturation vis-à-vis des puissances CPU afin de pouvoir tirer pleinement partie de la diminution des prix du hardware à puissance multipliée.

L'utilisation des annuaires devrait permettre :

- la fusion des annuaires spécialisés (application, téléphonie, personnel …)
- la mise en place du SSO (Single Sign On)
- la mise en place d'un EKI (enterprise Key Infrastructure - par analogie à PKI)
- simplifier et automatiser des tâches administrative ennuyeuses comme l'installation des imprimantes sur les stations de travail (NDPS par exemple qui présente une certaine similitude de fonctionnement avec SIP)
- faciliter la mise en place de VOIP (inscription des adresses AOR et URI)

Les applications d'abord : pas tout à fait !

Si on interroge des responsables business sur ce qui est le plus important dans l'informatique de l'architecture où des applications, ils répondront à 85 % les applications bien sûr !

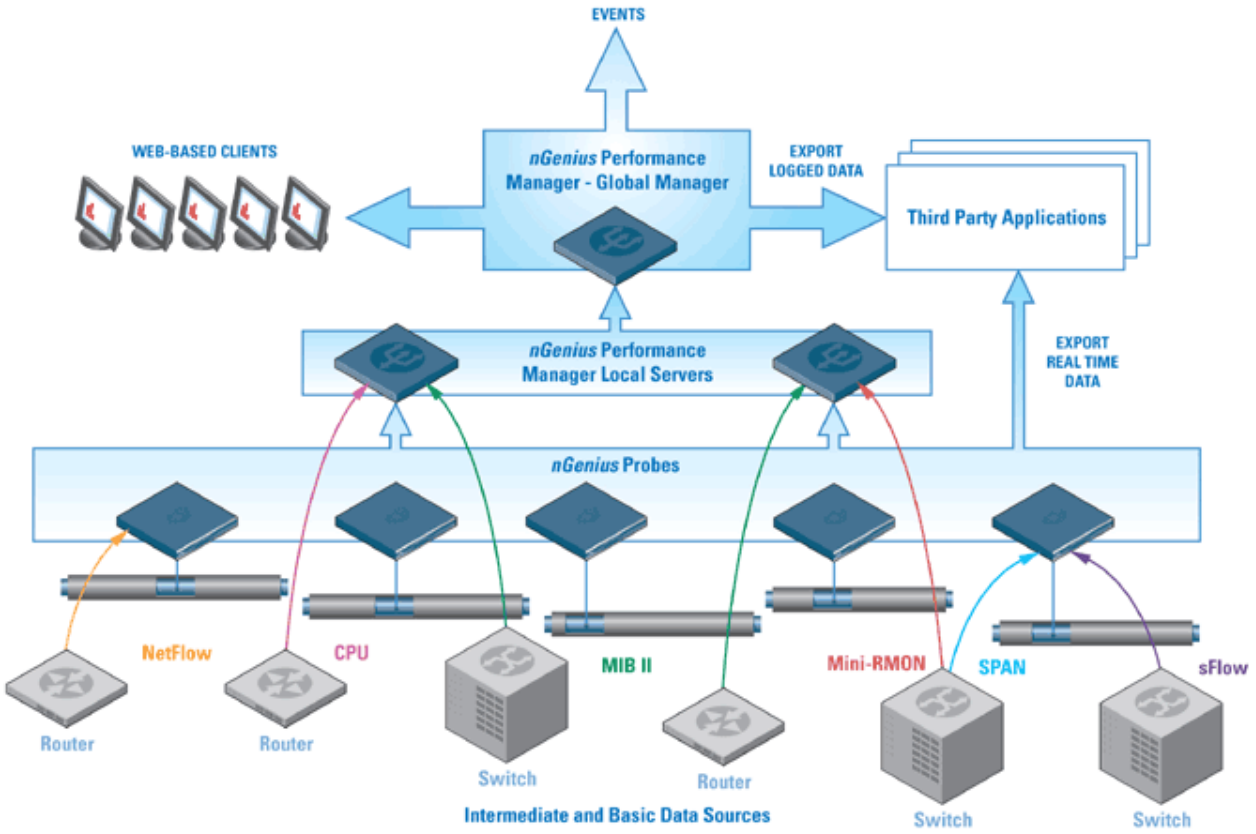
Et c'est vrai que sans application, l'informatique ne sert à rien, à part amuser les informaticiens.

Le problème est que ces applications ne doivent tout de même pas être hors de prix ni poser un hack sur l'entreprise !

Le fait est que la stratégie de l'entreprise devrait être de développer une architecture dont elle est maîtresse (conceptuellement) qui servent de cadre pour accueillir des applications qui devront se poser à un certain niveau, c'est à dire, qu'on ne leur permettra pas de s'ancrer profondément dans l'architecture pour pouvoir les faire évoluer facilement, ne pas être dépendant et pouvoir investir de façon incrémentale dans son système d'information.

C'est le contraire quasiment qui est fait aujourd'hui, par simple méconnaissance, ou à la suite de jugements « Rambo » à l'emporte pièce : « faut que ça marche, le reste on s'en fout ! »

Performance manager (Netscout nGenius)



Le message sous-jacent : suivre un incident en profondeur en faisant une coupe à travers les niveaux.
Pour lutter contre syndrome : « à mon niveau, tout va bien, ça vient pas de chez nous ! »