Déploiement et supervision d'infrastructure réseau

6, rue du Manège
54000 NANCY
FRANCE

pascal@rodmacq.com
www.rodmacq.com

00 33(0)3 83 35 39 33

Pascal Rodmacq - Avril 2006

Introduction

Infrastructure réseau : de + en + à prendre au sens large !

Qu'attend-on d'une infrastructure réseau ?

Commencer par l'existant !

Objets physiques, logiques, concepts, anticipation, pérennité.

Encore un modèle en couches !

Infrastructure réseau : ?

Le terme de réseau est utilisé avec une acception de plus en plus en plus large. En fait lorsqu'on parle de réseaux dans une entreprise, on peut faire référence :

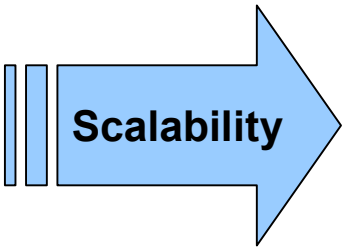
- **A une application sur une machine quelconque**
- **Aux services d'authentification**
- **Aux services de résolutions de noms**
- **Aux services de fichiers**
- **A la messagerie interne**
- **A la messagerie internet**
- **Aux services web internes**
- **A l'accès internet**
- **Au réseau local d'un site**
- **A l'accès à un autre site de l'entreprise**

Il est patent que dès qu'un des services ci-contre ne fonctionnera pas on entendra dire : « il y a un problème sur le réseau ?»

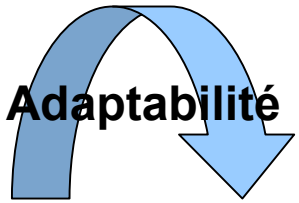
Déployer une infrastructure réseau aujourd'hui c'est mettre en place une 'infrastructure' qui va garantir :

Que les items de la liste précédente ont la plus grande probabilité d'être fonctionnels.

Que cette infrastructure sera largement 'automatique', c'est-à-dire qu'elle ne nécessitera pas une armée de personnel qualifié pour être maintenue en opération.



Qu'elle sera capable de supporter un certain changement quantitatif sans modification, ni achat, ni personnel supplémentaire. (plus de postes, plus de volumes, plus de serveurs, plus d'utilisateurs, plus de sites …)



Qu'elle sera capable de supporter un certain changement qualitatif (de nouvelles applications) sans une remise en cause radicale de son design, des équipements, des types de lignes, des débits …

Le déploiement d'infrastructure …

aujourd'hui, dans l'immense majorité des cas, se met en œuvre sur un existant !

Toute entreprise d'une certaine importance est en présence d'une infrastructure existante avec une histoire de 10 à 25 ans … en augmentation tous les ans !

Vous aurez toutes les chances au cours de votre carrière d'exercer vos talents à partir d'une situation héritée.

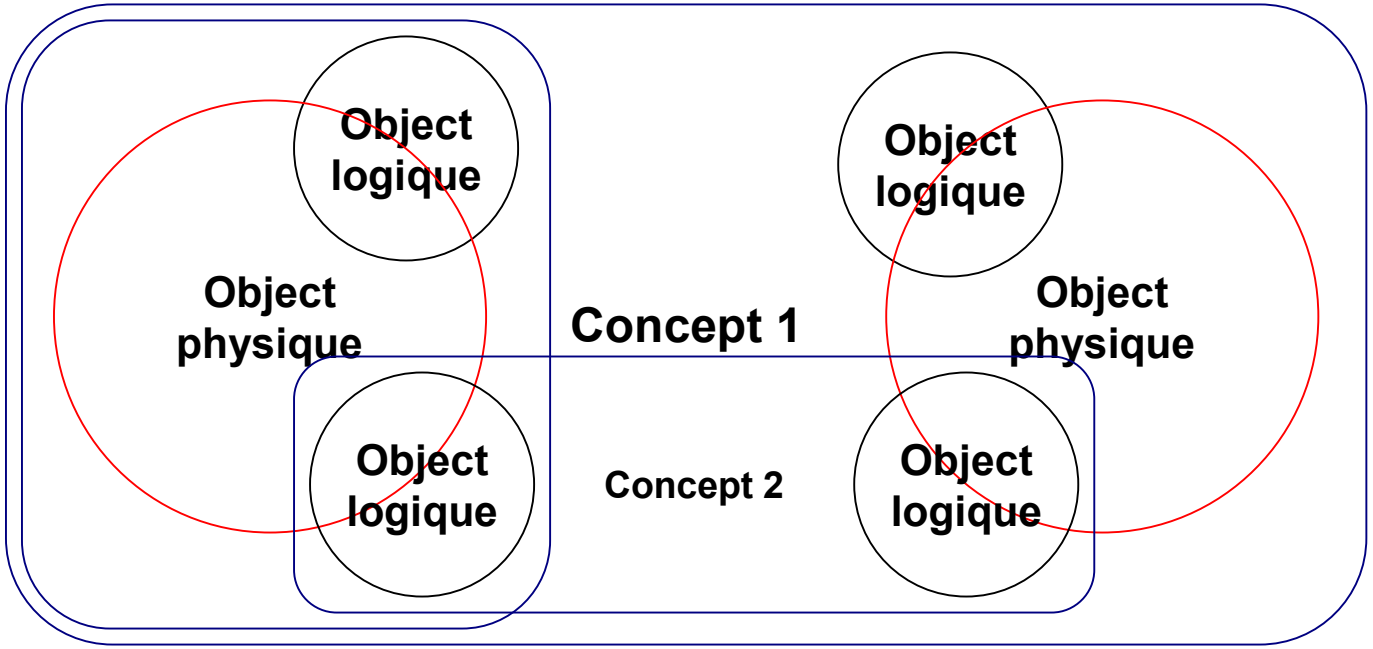
Une des tâches préliminaires à tout déploiement est la connaissance et la vérification de la documentation de l'existant. Le + souvent cette documentation est très déficiente !

Les occasions de travailler sur du neuf relatif :

- les locaux neufs, et notamment usines et entrepôts
- la bascule vers de nouvelles technologies : fibre, wireless

Le déploiement d'infrastructure …

implique de gérer des objets physiques et des objets logiques, les uns et les autres faisant référence à des concepts sous jacents qui peuvent être communs à un sous ensemble d'éléments et spécifiques à d'autres.
Il est important d'avoir une représentation mentale claire des relations entre ces éléments.



Approche de l'infrastructure par :

- niveaux
- objets physiques
- objets logiques
- concepts
- anticipation/pérennité

	Objets Physiques	Objets Logiques	Concepts	Anticipation / Pérennité
1	Connecteurs cables baies hubs switchs	Site LAN Campus	Topologie Plan Bande passante	Mois-Semestre / 15-20 ans
2	Adaptateurs Hubs Bridges Switchs	MAC Trame CSMA 802.x STP QoS ARP DLC	Espace de collision et de broadcast VLAN	Mois-Semestre / 4 - 6 ans
3	Routeurs Firewall Proxy PABX IP	TCP SNA IPX RIP OSPF BGP MPLS VPN NAT SOCKS SIP H323 VoIP	Espace d'adressage Adresses privées Adresses publiques Opérateurs (telcos) AS / Frontière	1 - 3 ans Stratégique
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	/ 5-15 ans / historique
5	Postes de travail	Windows Linux MacOS NetPC	Environnement utilisateur	1 an / 4 ans

Niveau 1 : site

Objets Physiques	Objets Logiques	Concepts	Anticipation / Pérennité
Connecteurs cables baies hubs switchs	Site LAN Campus	Topologie Environnement Bande passante	Mois - Semestre / 10-15 ans

Une brique de base fondamentale

- Unité de gestion primaire
- Source d'information primaire
- Fiche de site => Configuration Management DataBase

Design à appuyer sur : topologie, environnement, besoin en BP

- Le câblage est très structurant !

Comprendre la structuration de l'offre

L'appel d'offre

- Etude
- Input et rédaction
- Choix et commande
- Suivi et recette

Une brique de base fondamentale -1

La notion de site est beaucoup plus importante qu'il ne paraît à première vue, c'est une source d'information primaire et une unité de gestion de base du management réseau (et d'autres services de l'entreprises).

Documenter chaque site de son réseau est une tâche fondamentale qui ne doit pas être prise à la légère et qui aura son importance dans toute la chaîne de déploiement / support / gestion du changement et ce pour tous les niveaux.

La « fiche de site » devrait idéalement être conservée sous un format XML au niveau de l'annuaire de l'entreprise de façon à : être accessible par le système de management réseau, par tout service, s'exporter de façon sélective sur un format standard, admettre une information variée (les plans par exemple …)

Lorsque l'on doit intervenir sur un site (neuf ou dans le cadre d'un aménagement) il faut en profiter pour créer, ou mettre à jour la documentation. Celle ci doit comprendre les plans des locaux.

Les informations recueillies ne serviront pas seulement au niveau 1 mais aussi pour la sécurité, la maintenance, les appels d'offres (câblages, actifs, telcos), le déploiement …

Exemple vécu : le support d'un opérateur appelle un site, n'obtenant pas de réponse, le ticket est mis en stand by. Comment peut on expliquer cette situation comment aurait-elle pu être évitée ?

Une brique de base fondamentale - 2

Exemple vécu – réponse :

L'appel a eu lieu à 3h12 AM. Le site est une agence commerciale …

Exemple d'utilisation de la fiche de site

Dans le cadre d'un déploiement en mode projet c'est typiquement la fiche de site qui servira de référence à votre fournisseur pour accéder au site et notamment lui fournir un contact local.

Dans le cadre d'une maintenance tiers c'est la même fiche de site qui servira au fournisseur pour savoir comment qui, quand appeler pour vérifier un équipement ou livrer un équipement de rechange au milieu de la nuit sur un site industriel … et la procédure pour y accéder (identification de la personne, enregistrement du mouvement …)

Utilité des plans

Au niveau de l'étude
Au niveau de l'appel d'offre
Au niveau d'un déploiement
Au niveau d'une maintenance

C'est le plan qui servira a identifier l'implantation des objets physiques

Exercice :
lister quelques informations de la fiche de site

•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•
•	•

Le point d'entrée conceptuel pour la gestion des objets physiques de niveau 1 est la notion de topologie.

Exemples de sites :

200 m2 de bureaux, un entrepôt, 3 étages de bureaux, un immeuble, un ensemble d'immeubles, une usine avec divers bâtiments administratifs et de production. Dans ces derniers cas, on parlera de campus : une aire contiguë privée.

Les paramètres déterminants :

- Nombre de plateaux et disposition

3 plateaux superposés de 150 m2
3 plateaux de 120 à 500 m2 sur un campus de 8000 m2

- Densité de prises par plateau en nombre de prises par m2

- Environnement, accès, type d'exploitation (5/7 H8, 7/7 H24)

Bureaux, production, ville, campagne, ouvert (public), fermé (centrale nucléaire), friendly, hostile (éléctro-magnétique, toxique …), particuliers (Palais de l'Elysée, Tour Eiffel …)

Etude site : organisation et information

Identifier et informer les personnes concernées / utiles / nécessaires

- Responsable du site (Chef d'Etablissement)
- Responsable de la sécurité groupe / site
- Responsable de la maintenance
- Correspondant informatique site

Le volet sécurité doit être incorporé au projet dès son initiation. Par exemple le responsable sécurité SI du site doit être formellement informé et on doit définir avec lui les points de validations. (Exemple de problème typique : positionnement de prises réseaux sur une aire accessible à des visiteurs en attente …)

Inventorier ce qu'on sait et identifier ce que l'on ne sait pas du site

- nature de l'activité, mode d'exploitation
- utilisateurs (réels et : comptes génériques par exemple)
- boites aux lettres de messagerie (boites utilisateurs et fonctionnelles)
- équipements réseaux (postes, imprimantes, actifs LAN)
- équipements télécoms (routeurs, PAD, modems
- liste des lignes lignes télécoms (RTC, RNIS, LS)
- liste des applications
- pour tout cela il faut identifier les fournisseurs, les interlocuteurs chez ces fournisseurs, commerciaux et techniques, les contrats de location et de maintenance.
- les plans cotés des locaux
- les plans du câblage existant

Etude site : aspect technique

Le câblage est un élément très structurant, avec une forte pérennité.
La fiabilité ne doit plus être questionnée une fois le câblage mis en service et on ne s'attend pas à ce que le design soit remis en cause avant le long terme.

Identifier normes et contraintes

. Vient d'une étude qui relève de la couche liaison de données en terme OSI
. Une norme est choisie : par exemple Gigabit Ethernet.
. Une fois la norme choisie, elle définie d'elle même un certain nombre de contraintes sur le câblage dont il faut prendre connaissance et qu'il faut logguer. Ces contraintes portent sur la nature des supports utilisables, la qualité de ces supports, des connecteurs, les règles de raccords câble/connecteurs, les longueurs maximales en fonction du support et du nombre de ruptures.

Confronter les contraintes à la réalité et à vos buts

. Il faut assimiler ces contraintes mentalement et les confronter à la topologie des lieux, d'abord sur les plans cotés des locaux.
. Le câblage existant est-il en accord avec avec les normes retenues ?
. Etudier les plans du câblage existant le cas échéant.
. Identification l'ancien câblage à démonter le cas échéant.
. Identifier l'implantation des prises existantes et nouvelles souhaitées.
. Identifier l'implantation des baies.

Le passage en revue des points ci-dessus doit permettre de préparer la visite de site qui devra valider les plans, les emplacements possibles des baies et prises.

Etude site : visite interne

Une première visite de site doit avoir lieu avec les personnes identifiées au début du projet mais sans les fournisseurs.

Par exemple une visite sur un site industriel se fera typiquement avec : outre le correspondant informatique local, un responsable maintenance (électricité, automatisme, passage de câble), un responsable production (contrainte d'accès, d'interruption, plage de travail, arrêt programmé …), un responsable qualité et sécurité. Vous devez disposer de la personne capable de vous renseigner sur la future disposition des accès réseaux qui peuvent dépendre de travaux ou de changements d'implantation non encore réalisés (déménagement d'un service, nouvelle disposition d'un entrepôt, mise en place d'une nouvelle machine …)

C'est l'occasion de vérifier les dépendances entre le projet de câblage et les projets du site … qui seront des contraintes à incorporer pour la réalisation de votre planning. La visite est souvent l'occasion de découvrir des choses absolument ignorées de tous sauf du site (réseau d'automates local par exemple …). C'est l'occasion de faire vérifier l'équi-potentialité des masses entre les bâtiments.

La visite doit se faire plateau par plateau, plan en mains, crayon, gomme … s'il n'y a pas de plan, c'est le moment de les tracer à main levée ! (il ne faut pas prendre cela à la légère)

La visite doit être suivi d'un debriefing immédiat où seront récapitulées les observations, les décisions, les non-décisions, les questions à arbitrer … tout cela fera l'objet d'un compte rendu écrit (mail) qui aura valeur de cahier des charges interne.

Etude site : cas d'une nouvelle technologie

Si on change radicalement de technologie pour choisir quelque chose qui n'est pas encore très répandu sur le marché, on entre dans un autre mode de fonctionnement où l'étude préalable va être beaucoup plus longue et devra faire l'objet d'un planning en soi.

Par exemple à ce jour le déploiement d'une solution Wireless à peine ambitieuse va requérir une étude et une planification très conséquente.
Par exemple, les considérations relatives à la sécurité vont être tout de suite plus étoffées.

Le comportement des ondes dans la géométrie des locaux n'est pas encore quelque chose de bien dominé, (on est en 3D, on ne parle plus de plateau mais de volume) aujourd'hui cela nécessite une étude au cas le cas.

En Wireless il faut savoir si on veut traiter les utilisateurs dans la mobilité : doit-on ou veut-on traiter le roaming ? Si oui il faut définir les aires de roaming acceptables (seamless roaming).

Ces décisions auront un impact sur les couches supérieures. On ne peut pas concevoir un roaming entre des réseaux (au sens IP) différents par exemple ! Il faut concevoir un backbone IP unique pour le roaming inter buildings … Pour cela il faudra selon toute vraisemblance recourir à un VLAN qui assurera un point de présence sur chaque bâtiments …

Une nouvelle technologie peut bouleverser les raisonnement au delà de sa sphère d'application APPARENTE (car on ne saisie pas instantanément les implications comme avec une technologie qui nous est familière).

Comprendre la structuration de l'offre -1

Au cours des années 70/80, on parlait de systèmes de câblage en référence à des offres propriétaires. Le signifié a évolué au fil du temps de la façon suivante :

•Une offre de constructeur informatique indissociable de ses machines et de ses équipements et systèmes : BCS, ICS, DCS.

•Une offre issue des téléphonistes dont Systimax d'ATT est l'exemple N° 1, maintenant LUCENT. (Pour mémoire aussi le cas particulier du 120 ohms de FT)

•Une offre spécifique au monde réseau (Cabletron) associé à une offre d'actifs.

Le business model fondé sur une intégration verticale plus ou moins profonde est obsolète. Notons toutefois qu'il a tendance à se reformer spontanément - quoiqu'à une échelle microscopique - lorsque la technologie est pointue et encore confidentielle (wireless pour des réseaux conséquents.)

A ce jour il y a une offre horizontale des composants de base : tous les composants de base du câblage (câble, connecteurs, panneaux, baies - le matériel actif n'est plus inclus dans le système de câblage) sont accessibles individuellement à un grand nombre d'acteurs de façon indifférenciée : c'est la conséquence des standards sur l'organisation du marché.

Dans ce contexte les fabricants du matériel de base ont repris un certain pouvoir en développant une politique de marque et d'agrément.

Enfin, depuis le début des années 90, la technologie Ethernet s'est imposée comme un véritable monopole de fait. Les normes de câblage associées sont donc devenues très communes et très bien dominées par les fournisseurs. On câble typiquement avec en tête les requirements pour la dernière version d'Ethernet

Comprendre la structuration de l'offre -2

L'offre commerciale

L'offre commerciale est très variée, se situant autour des grands noms de la téléphonie, de quelques grands spécialistes du câblage pur (Expert Data), des fournisseurs de matériel actif, d'innombrables SSII, des grands constructeurs qui supportaient un système de câblage maison (IBM BULL DEC) et ont créé un département réseau. Tous s'appuient maintenant sur les standards normés.

L'offre de réalisation

La réalisation du câblage à proprement parler repose sur d'une part un tissu d'entreprises locales spécialisées en courant faible et historiquement issues de la téléphonie, d'autre part quelques petites entreprises spécialisées dans les tests ou la fibre, le sans fil, qui travaillent en sous traitance pour les sus-nommés. Ils constituent le goulet d'étranglement en matière de réalisation de câblage. Les chantiers de câblage démarrent souvent en retard et la cause principale en est que l'entreprise avec qui vous avez traité a pris des engagements de délai sans assurance de la disponibilité de son (ses) sous traitant(s).

La qualité de réalisation est en générale excellente et elle a progressé au cours de 10 dernières années. De plus, l'extraordinaire monopole de la technologie Ethernet allié à une tolérance beaucoup plus grande des adaptateurs diminuent considérablement les risques de problèmes sur le réseau.

Appel d'offre – consultation

Document initial de consultation

- **les plans cotés des locaux avec un nommage des lieux.**
- **les plans du câblage existant le cas échéant**
- **l'identification de l'ancien câblage à démonter le cas échéant**
- **l'implantation des prises souhaitées**
- **les normes techniques de câbles, de prises**
- **les longueurs maximales de tronçons : fibres et cuivre**
- **les contraintes éventuelles de positionnement des baies de brassage**

Instructions pour présenter la réponse

-**Schéma d'implantation : emplacement des baies, le nombre de prises par baies, les chemins et le nombre de brins entre baies.**
- **un schéma de chaque baie montrant la disposition des panneaux le nombre d'unités occupées / disponibles**
- **demander une réponse avec métrique et chiffrage baie par baie (pas d'agrégation) et infrastructure tronçon par tronçon.**
- **demander à séparer le coût matière et le coût main d'œuvre, demander les durées.**
- **donnez une date limite de remise de proposition**

Dans un premier temps lancer une consultation sur typiquement 3 fournisseurs en leur prodiguant les données et instructions ci-dessus et en les convoquant à une visite de site. Ne vous préoccupez pas de fournir un planning ni des contraintes d'accès site, sécurité etc … pour le moment.
La visite de site est très importante, elle doit se faire avec un homme de l'art et vous devez lui laisser du mou pour s'exprimer, et proposer des solutions auxquelles vous n'auriez pas songé.

Appel d'offre - dépouillement choix

Visite de site

Débriefez chaque visite de site avec vos collègues, confrontez vos impressions, notez vos remarques, rappeler le CR du débriefing précédent.

Réception des propositions / dépouillement

Relancer à l'approche de la deadline si nécessaire.
Vérifier la conformité de la réponse par rapport aux standards demandés, aux quantitatifs et à la présentation.
Faites vous envoyer les propositions, évitez la sempiternelle remise de la main à la main, vous avez surtout du temps à y perdre.

Ensuite le principe consiste à diviser pour régner en établissant des comparaisons postes par postes et transversales.

Exemples

Comparer le métrage câble / fibre total de chaque proposition (attention aux options)
Comparer un ratio général de coût par prise (total général / nombre de prises)
Comparer le coût par prise plateau par plateau avec baie et sans baie
Comparer le coût de la fibre général / par rapport au métrage proposé
Refaire les mêmes calculs avec et sans main d'œuvre

Tout ceci doit faire apparaître les éventuels incohérences.
Posez vos questions ! Ne restez pas sur votre faim ! Faites jouer les différences, obtenez des ajustements par téléphone et notez les sur la proposition.

Appel d'offre - négociation finale

Repassez en revue la proposition point par point avec le fournisseur choisi

En fait à ce stade tout doit déjà être clair pour vous.
Si des incohérences avaient été noté les rappeler.
Arrêter le choix des options.
Viser le contenu du cahier de recette :
Repérage vérifié - Test prise par prise (appairage, affaiblissement, para diaphonie)
Etablir le délai de remise du cahier de test après la fin du chantier
Etablir un délai de remise en conformité pour les prises qui ne seraient pas aux normes

Introduire le planning, les délais

Demander qui câble !
S'il s'agit d'un sous traitant demander à savoir s'il est déjà réservé pour votre chantier.
Demander qui fait les tests !
Demander si la fourniture (câble, prise, baie) est disponible, d'ou elle vient ?
Sur stock, commande ? A qui ?
Toutes ces questions permettront de verrouiller la vraisemblance des engagements de délais.

Etablir son propre bon de commande

Avec vos termes et tout ce qui n'était pas spécifié sur le document du fournisseur.
Il faut clairement faire établir vos conditions d'achats et ne pas signer sur un document portant en générale les conditions de ventes au verso en petits caractères.
Cette précaution pourra éviter des complications à l'avenir car il n'y aura pas acceptation croisée et simultanée de conditions de vente de la part de l'acheteur et de conditions d'achat de la part du vendeur.

Suivi de chantier

Une fois un fournisseur choisi, il est important d'être solidaire avec lui et de l'aider dans la réalisation de sa tâche.

Donnez lui toute l'information nécessaire
Préparez son accueil sur le site
Pour un chantier important, l'équipe constituée en début de projet se charge de l'accueil des représentants du fournisseur dans une réunion préparatoire, fait visiter le site, donne un recueil des règles d'accès, sécurité, circulation, réception des marchandises …

C'est la que se décide la périodicité des réunions de chantier et les personnes devant y assister.

Vérifier qu'une organisation de chantier se met en place, qu'un pipe de communication existe et fonctionne (par exemple vous devez recevoir une information sur la date de la prochaine réunion de chantier)

En fonction de la durée prévue du chantier et de sa criticité, établissez quelques jalons où vous rendrez sur place (1/4 1/3 ½)

Note sur la garantie constructeur / câbleur

Un système de câblage lambda d'un fournisseur donné repose sur une chaîne comprenant le câble (peu de constructeurs), les connecteurs, les panneaux et cordons de brassage.

Une offre de câblage (type Lucent) est souvent associée à une garantie constructeur d'une quinzaine d'années, à condition que le câbleur n'utilise que des éléments en provenance du dit constructeur et certifie son chantier à travers la procédure constructeur. En pratique, la garantie constructeur est souvent évoquée au niveau de la négociation commerciale, mais pas toujours livrée formellement au client !

Souvent à cause de la lourdeur de la procédure ou parce que l'entreprise commanditaire, qui dispose de l'agrément n'a pas su transmettre les instructions nécessaires à son sous traitant et n'a donc pas recueilli les informations nécessaires en temps utile, ou a fait preuve de négligence ou parce qu'il est habitué à ce que le client ne le demande pas … Cela ne veut pas dire que le client ne dispose pas d'une garantie légale, cela signifie que ce n'est pas celle du constructeur.

A contrario, le fait de livrer cette garantie constructeur avec la recette est le signe que le chantier a été mené avec rigueur et que le commanditaire a une relation bien établie avec son sous traitant.

Si votre choix s'est porté sur un constructeur qui prodigue ce service, il faut en exiger la délivrance par votre fournisseur et établir une clause de rétention au niveau de votre document de commande tant que le certificat de conformité n'est pas délivré.

Pascal Rodmacq - Avril 2006

Niveau 2 : espace de broadcast

Objets Physiques	Objets Logiques	Concepts	Anticipation / Pérennité
Adaptateurs hubs switchs Bridges	MAC Trame CSMA 802.x STP QoS ARP DLC	Espace de collision et de broadcast VLAN	Mois - Semestre / 4-6 ans

Rappel du concept d'espace de broadcast

Définitions

- **Espace de collision / de Broadcast**
- **Routing switch & switching router**

Inventorier et documenter l'existant

Choisir un niveau de standard supporté

Gérer l'hétérogénéité

Cas des protocoles non routable

Définir une politique de maintenance dérivée du design

Point d'entrée conceptuel : espace de broadcast

L'ensemble des adaptateurs réseaux recevant une trame de broadcast donnée définit un espace de broadcast.

Sur un brin Ethernet partagé l'espace de broadcast est égale à l'espace de collision. Dans une technologie entièrement switchée, on ne tient compte que de l'espace de broadcast.

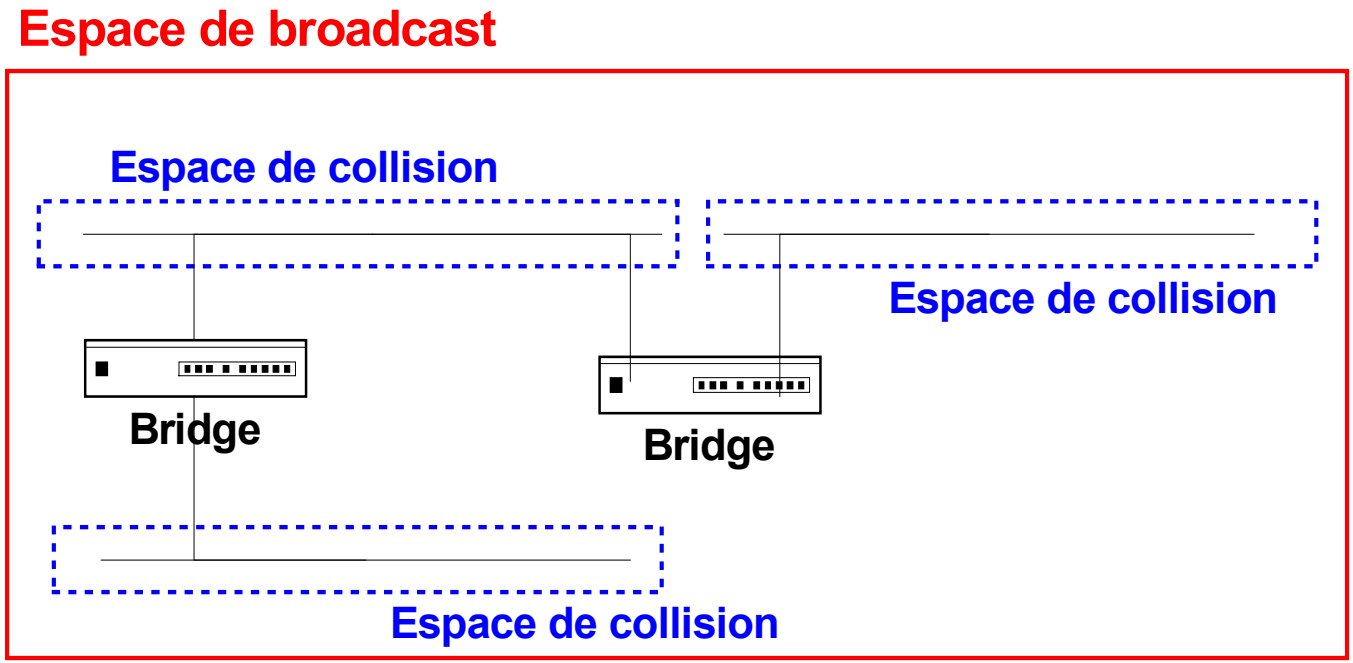
Le jeu consiste à limiter l'espace de broadcast à une taille raisonnable tout en permettant à chaque équipement d'accéder aux services du réseau.

Un maximum empirique pour cette taille, compte tenu des usages actuels, est 250 sur une technologie GE à moduler en fonction des cas marginaux.

Attention, ce chiffre ne reflète pas un nombre d'utilisateurs : il faut tenir compte de tous les équipements du réseau qui ont une adresse MAC : serveurs, imprimantes, Switchs, routeurs.

Un VLAN définit un espace de broadcast.
Un VLAN permet de rendre indépendant l'espace de broadcast de la géographie (les équipements ne sont plus nécessairement contiguë)
Les VLAN permettent de segmenter l'espace d'adressage.
Un équipement de niveau 3 est nécessaire pour faire communiquer 2 équipements appartenant à des VLANs différents.

Distinction : espace de collision / espace de broadcast



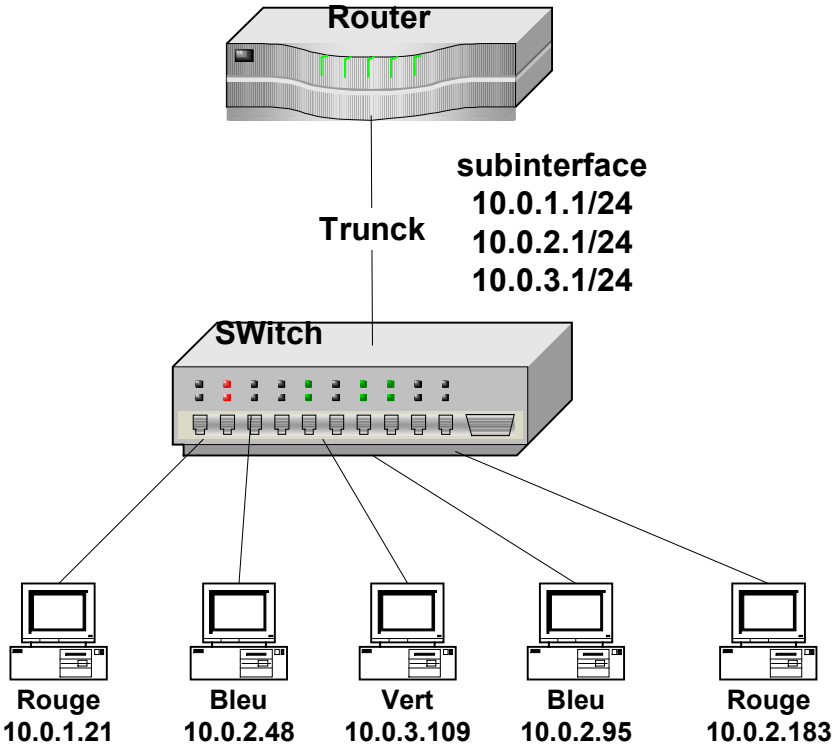
Les espaces de collision peuvent être limités par l'utilisation de bridges. Un switch peut être vu comme un bridge qui définit autant d'espaces de collision que de ports.
Premier switch apparu sur le marché : Kalpana EtherSwitch 1991 mais avant cela étaient apparus les bridges multiports …

Schématisation des espaces de broadcast

1 - Représentation fondée sur la disposition et les liaisons physiques des équipements.

Nous avons 3 VLAN :
Rouge : 10.0.1.0/24
Bleu : 10.0.2.0/24
Vert : 10.0.3.1/24

La représentation des switchs, ne permet pas de visualisation graphiquement les espaces de broadcast



Schématisation des espaces de broadcast

2 - Représentation fondée sur la disposition et les liaisons logiques des équipements du même réseau

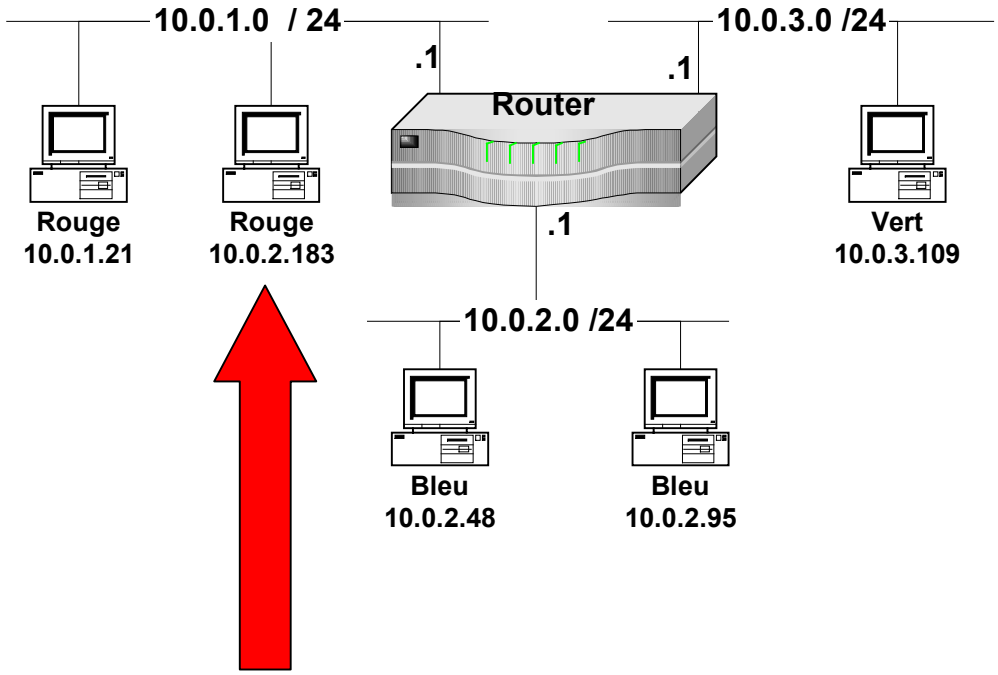
Les 3 VLANs :
Rouge : 10.0.1.0/24
Bleu : 10.0.2.0/24
Vert : 10.0.3.1/24

Apparaissent clairement

NB : 2 types de VLAN

SVL : Shared VLAN
1 table d'adresses MAC
1 instance de STP)

IVL : Independent VLAN
1 table / VLAN
1 instance STP / VLAN



Cette machine est mal placée, l'aviez vous remarqué sur le schéma précédent ?

Routing switchs et Switching routers

Depuis la fin de années 90 sont apparus des matériels hybrides dont le fonctionnement reste souvent confus dans l'esprit de la profession. En anglais, il y a le mérite d'avoir 2 expressions assez parlantes :

Routing switch

Fondamentalement un switch qui peut intégrer des informations supérieures au niveau 2 pour switcher une trame. Ces informations peuvent venir du niveau 3 ou même au delà, on parle de MLS Multi Layer Switching. Ce type d'équipement ne tourne pas un protocole de routage.

Attention : certain Routing Switch recréent une entête niveau 2 (et décrémentent le TTL du paquet) c'est à dire que le paquet semble provenir d'un routeur, d'autres pas : ils switchent une trame non modifiée.

Switching router

Fondamentalement un routeur qui peut switcher des paquets. Cet équipement supporte un (ou plusieurs) protocoles de routage il utilise cette information pour piloter le switching des paquets à travers un circuit dédié identique à celui qu'on trouve dans un switch.

Inventaire et documentation du niveau 2

Encore une fois, documentation et inventaire s'imposent comme tâches primaires. L'inventaire à ce niveau vise à faire ressortir :

- les technologies utilisées sur le site et les standards supportés, les technologie / débit, HUB Switch Capacité
- les marques/modèles importent peu.
- Exemple : SMCTiger 32T => Hub Ethernet 10BT 32 ports
- Les normes supportées : 802.3u (autoneg), 802.1D (STP), 802.1Q (SVL VLAN & IVL VLAN) …
- Les capacités en nombre de prises
- uplink : nombre / technologie / type de connecteurs
- Adresse de niveau 3, moyens de management primaires : Telnet, console (authentification)

La documentation doit permettre :

- de situer les équipements géographiquement
- de renseigner l'usage de STP et les instructions de choix du root bridge.
- d'identifier les VLANs
- d'identifier les espaces de broadcast (ce qu'elle fait très rarement)
- de lister les applications utilisant un protocole non routable.

Choisir un niveau de standard supporté

Spanning Tree

- rester sur STP classique ou passer à RSTP (Rapid STP 802.1w)
- RSTP permet de diminuer le temps de convergence
- mais l'élément prépondérant reste de limiter les domaine de broadcast et d'avoir un STP par DdB
- Le mieux : faire les 2 !

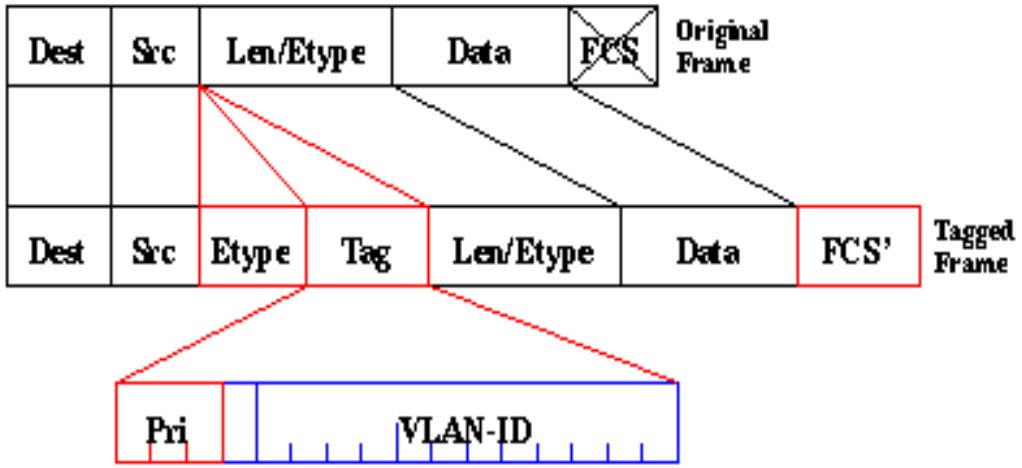
QoS or not Qos ?

A ce jour la question au niveau d'Ethernet est le support d'un niveau de qualité de service différencié. Ethernet, à la base un média partagé n'a jamais intégré cette problématique qui n'est typiquement pas sa philosophie.
Si on veut supporter VoIP au dessus de Ethernet avec un niveau de qualité minimum, c'est une précaution de s'assurer des switchs supportant 802.1p et 802.1Q. Toutefois, en l'absence de bande passante suffisante, toute prioritisation est vaine de toute façon …

Faire des choix et les documenter

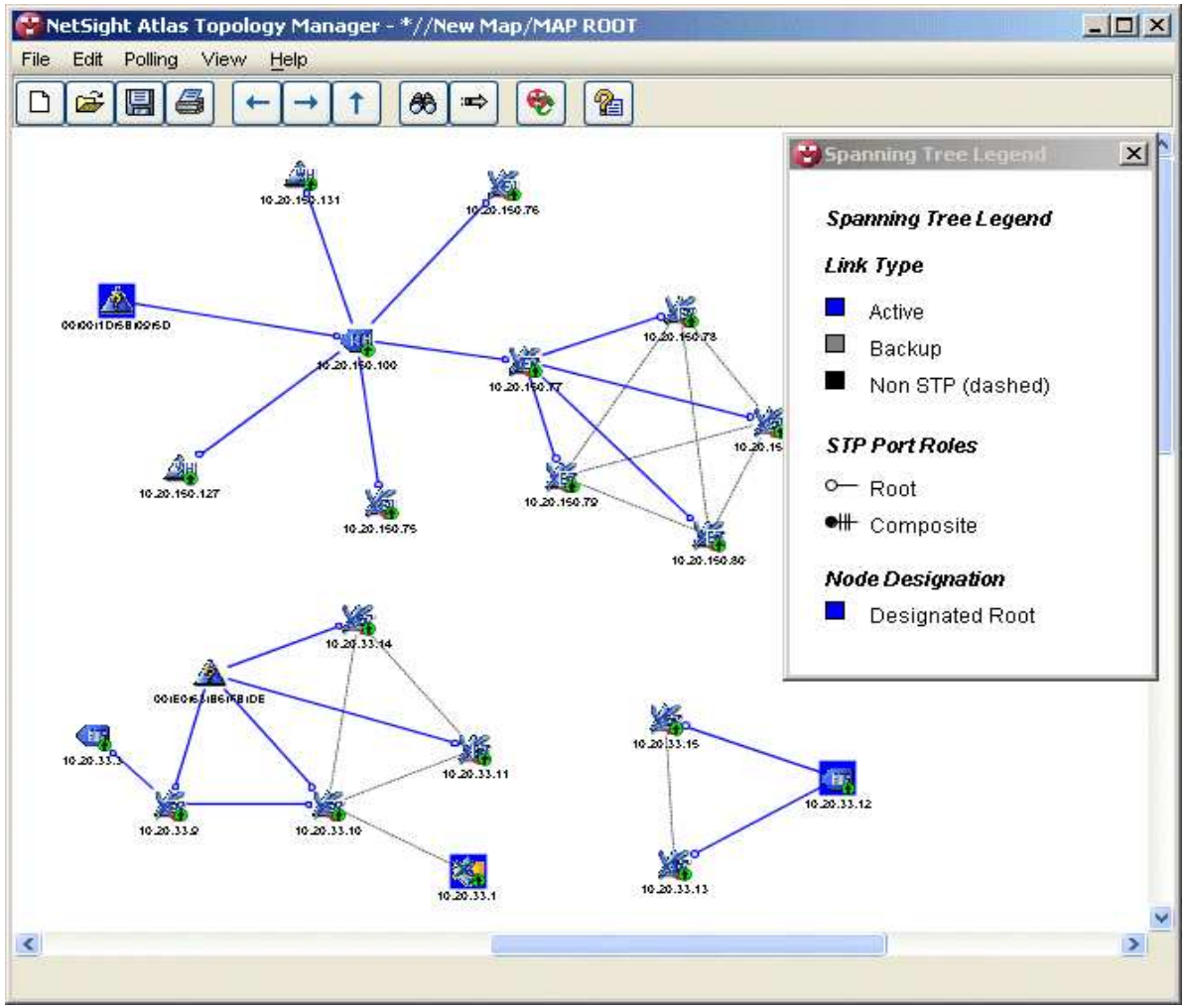
Quoi qu'il en soit, l'essentiel est de savoir ou on en est et d'être conscient des limites de son réseau pour pouvoir envisager le support en connaissance de cause d'une nouvelle application (comme VoIP)

Trame 802.1Q – cohabitation avec les bits QoS (802.1p)



A ce jour, les moyens de différencier les trafics sur Ethernet, en dehors d'une analyse des paquets, reposent sur la gestion des 3 bits définis par 802.1p permettant de définir, au niveau des switchs et routeurs et carte réseaux (qui gère : driver ou OS ?) une politique de queing (7 queues) « *je n'envoie pas une trame d'une queue de priorité donnée tant que il y quelque chose dans une queue de priorité plus élevé ou qu'un timer ait expiré (pour garantir qu'il n'y a pas d'attente infini)* »

Exemple de topology manager



Logiciel Enterasys Seuls les matériels du constructeur sont gérés. Toutefois une interface est prévue pour HP OpenView qui détient un quasi monopole dans le domaine.

Gérer l'hétérogénéité

Une des conséquences de ce qui précède est : une fois arrêtée une décision de supporter certains standards, que faire des équipements existants qui ne les supportent pas ou pas tous ?

Identifier questionner

- **La première étape est de les identifier**
- **Sont-ils en pleine propriété ? En location ?**
- **Sous contrat de maintenance ?**
- **Ou en sont-ils en terme d'amortissement ?**
- **firmware upgradable pour supporter les nouveaux standards ?**

Isoler / regrouper

- **garder ce type de matériel dans des groupes homogènes isolés et séparés du nouveau par un équipement de niveau 3 (routeur ou un switch routeur)**

Remplacer

- **Le travail de démontage, remontage, les perturbations associées dans le cadre d'un déplacement de matériel sont à mettre en balance avec la valeur résiduelle des équipements et leur pérennité.**
- **S'ils sont amortis, leur remplacement sera facile à envisager (ce qui est une façon de ne pas gérer l'hétérogénéité !**

Gestion des protocoles non routables

Définition

Un protocole non routable travaille par définition au niveau 2 et ne dispose pas d'adresse de niveaux 3. Pour que 2 équipements utilisant un tel protocole puissent dialoguer entre-eux, ils doivent appartenir au même espace de broadcast.

Exemples : NetBeui, LAT, DLC, Réseau industriel

Il est important d'identifier ces équipements ou applications.
LAT sera un équipement du domaine DEC – de + en + rare.
DLC sera un AS400 v3 par exemple ou une imprimante HP.
NetBEUI peut être imposé par d'anciennes applications ou de nouvelles applications ayant conservées d'anciennes couches !
Réseau industriel (très fréquent, très varié, très mal documenté)

Planifier / réagir

Si la découverte de ce type de protocole a été planifié, on peut réfléchir à une façon de s'en passer, en remplaçant le matériel ou en le réglant différemment.
Si la découverte se fait au moment ou l'équipement ne communique plus quand on le branche sur le nouveau réseau, on peut les mettre sur un VLAN fourre tout qu'on a gardé en réserve pour ce type de cas.

Echelle de complexité

En matière de LAN, la complexité croît exponentiellement avec le nombre d'utilisateurs et le nombre de plateaux.

Entre un site de 50 personnes ou tout le monde est sur une pile de 2 switchs et un campus de 5 bâtiments abritant 2000 personnes la nature même des problèmes est différente.
Le premier cas peut être traité par le premier néophyte venu et ne nécessite qu'un contrôle.
Le second cas réclame un traitement en mode projet avec une étape design conséquente qui implique la présence d'au moins un vrai connaisseur en la matière.
Attention il ne s'agit pas d'un spécialiste des switchs X, la bonne personne pourrait n'avoir jamais mis les doigts sur l'interface d'un switch.
La mise en œuvre ultérieure réclamera effectivement des spécialistes des matériels choisis.
Vous devez vous assurer que le chargé du design domine les concepts expliqués ci-avant et vous devez vous y impliquer pour garantir que le design choisi sera en accord avec vos priorités et vos choix.

Le responsable du design ce doit être vous !

Définir une politique de maintenance

L'achat d'actif en tant que tel ne pose pas de problème, dès que l'on est capable de spécifier ses besoins.

Plus délicat est la définition de sa politique de maintenance et le fait de savoir si l'on doit ou non prendre un contrat de maintenance sur les équipements de niveau 2. Mais le vrai problème à propos du contrat de maintenance n'est pas tant de savoir si on doit en prendre un ou non, mais d'en définir le contenu et le cas échéant, d'être capable de l'activer en cas de besoin au niveau local.

Notez par exemple qu'un contrat de maintenance style remplacement de l'équipement défectueux sur site ne sera pas suffisant pour garantir la remise en service de votre réseau si on ne sait pas comment configurer l'équipement en fonction de vos paramètres => la documentation fait partie de la politique de maintenance.

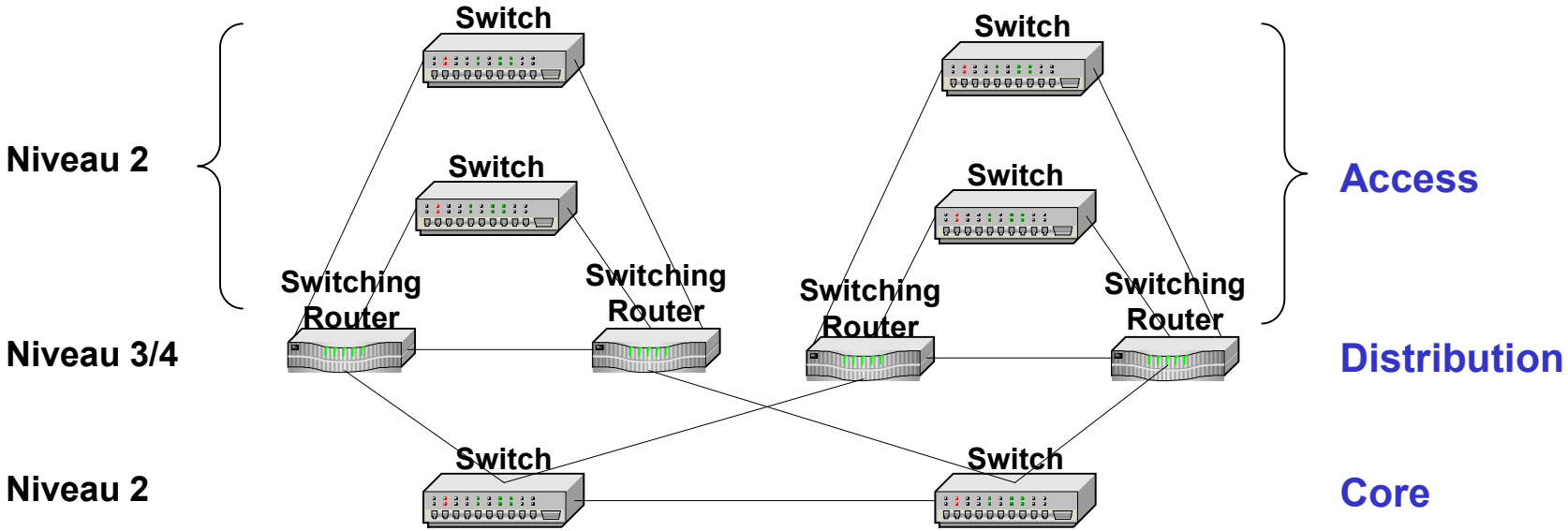
Enfin, il faut toujours au minimum plusieurs heures pour se faire livrer un équipement. Si le réseau dépend de cet équipement peut-il rester hors service tout ce temps ?

Pour du matériel sophistiqué, le délai peut être beaucoup plus long, et seule une société de maintenance peut garantir la disponibilité sous un délai acceptable.

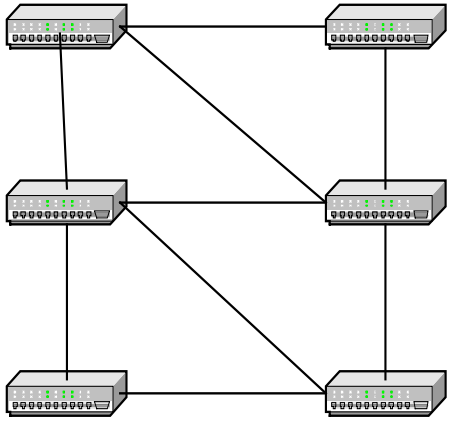
C'est donc le design, en incluant une certaine redondance, qui garantie le niveau de résilience souhaité car rien ne pourra réduire le délai de remise en service d'un équipement en panne à 2/3 heures si on ne dispose pas de la pièce en local.

En adoptant un design hiérarchisé par niveau, on associe aux équipement d'un niveau donné un degré de criticité et une politique de redondance et de maintenance.

Exemple de design à 3 niveaux (campus)



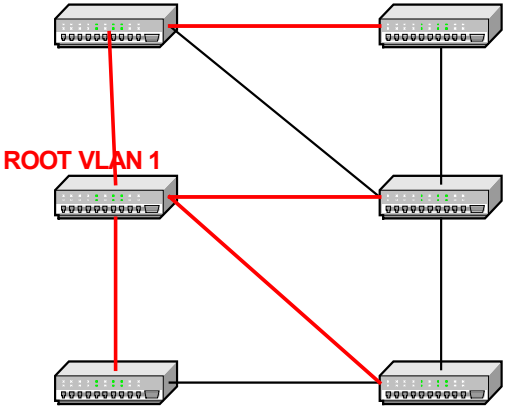
Spaning tree, VLANs & load balancing



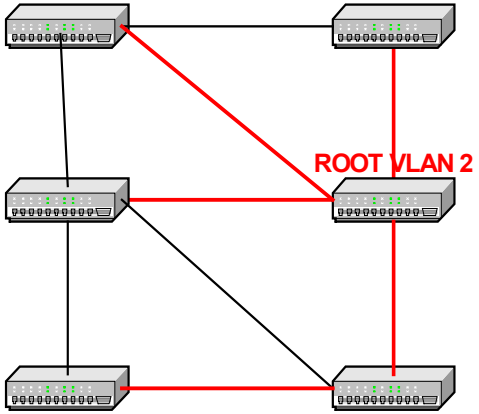
Cet exemple montre comment l'utilisation d'une instance de spaning tree par VLAN associée au placement raisonné du ROOT Bridge permet de pratiquer du load balancing sur tous les liens du réseau.

Si le ROOT avait été placé au même endroit pour les 2 VLANs, 4 des liaisons n'auraient jamais été utilisées.

Liens activés pour VLAN1



Liens activés pour VLAN2



Définir une politique de maintenance

Quelques paramètres à considérer

- taille, complexité, criticité du site (que se passe-t-il si ? = enjeu)
- présence ou non de personnel qualifié sur site
- ratio coût maintenance / valeur de l'équipement
- gestion des informations de configuration de l'équipements

Petit site à un espace de broadcast (moins de 100 utilisateurs)

- gérer la panne par procédure en vous reposant sur des capacités en spare (pile de 4 switchs la ou 3 auraient suffit)
- le site doit disposer d'une procédure pour le remplacement du matériel défectueux et sa remise en service (affectation d'adresse, activation de telnet …)
- en fonction de ce que vous voulez gérer, un contrat de maintenance basique peut couvrir le remplacement de l'appareil défectueux et son re-branchement sur site.

Site à 2/4 espaces de broadcast

- **Hiérarchiser les équipements : distribution / access**
- le niveau distribution sera redondé
- le niveau accès sera sparé on line (comme les petits sites) ou off line

Au delà

- **Hiérarchiser les équipements sur 3 niveaux core / distribution / access**
- Le niveau core sera obligatoirement redondé (critique)
- Le niveau distribution sera redondé ou sparé suivant la criticité
- Le niveau access sera sparé off line (équipement en spare sur site)

Métrologie réseau sur niveau 2

Le niveau 2 est une source d'information primaire pour l'analyse du trafic réseau.

En capturant des trames au niveau 2 on est capable d'analyser l'ensemble des problématiques réseaux en remontant dans les couches.

Pour avoir une vue exhaustive, il faut poser une sonde sur chaque espace de broadcast.

Le problème peut ne pas être simple dans un réseau avec un grand nombre de VLANs, souvent on choisit un point central où on suppose que l'ensemble du trafic doit converger.

La solution est de considérer ses schémas de représentation des espaces de broadcast et de placer les sondes en connaissance de cause.

Sur les switchs, il existe en général un port sur lequel on peut cloner l'ensemble du trafic, on peut ainsi collationner le trafic de tous les VLANs transitant par ce switch, par contre l'analyse des données peut être compliquée ultérieurement.

Choisir et identifier ces points de collecte est un bon départ si l'on doit superviser finement son trafic réseau (le jeu n'en vaut la chandelle que sur des sites de type campus)

Même si on ne doit pas faire de supervision niveau 2, l'identification de ces points doit faire partie de la documentation du niveau 2, ceci permettra de savoir ou brancher un analyseur de trames et ce qu'on est censé y trouver si l'on doit faire du troubleshooting sur le réseau.

Niveau 3 : réseau - plan d'adressage

Objets Physiques	Objets Logiques	Concepts	Anticipation / Pérennité
Routeurs **Firewall Proxy PABX IP**	**TCP SNA IPX RIP OSPF BGP MPLS VPN** **NAT SOCKS SIP H323 VoIP**	**Espace d'adressage Adresses privées Adresses publiques** **AS / Frontière Opérateurs (telcos)**	**1 - 3 ans Stratégique / 5-15 ans / historique**

La préparation du plan d'adressage est une des tâches fondamentales de tout déploiement réseau, elle l'est d'autant plus qu'à ce jour TCP/IP est hégémonique. (nous nous référerons essentiellement à ce protocole)

Panorama historique

Fondamentaux pour l'établissement du Plan d'adressage

Documenter l'existant

Panorama historique

Avant TCP, le protocole le plus répandu sur les LAN était IPX (on trouvait aussi DECNet et AppleTalk). IPX avait la particularité d'être entièrement automatique, il n'y avait qu'une chose à configurer : une adresse réseau par espace de broadcast !

Avec l'arrivée de TCP, les entreprises n'avaient pas la culture «adresses» et découvraient qu'il fallait numéroter chaque interface, ceci a donné lieu à un joyeux désordre dont les traces subsistent encore aujourd'hui !

De plus, le premier réflexe des grandes entreprises dans les années 90, sur rumeur ambiante de pénurie prochaine d'adresses IP a été de réserver des plages de classes publiques (B pour la plupart et parfois C) auprès de l'InterNIC et de numéroter leurs stations de travail en statique avec ces adresses.

Lorsqu'elles sont arrivées au bout de leurs adresses au milieu des années 90, notamment parce les postes de travail remplaçaient les terminaux, elles ont déployé NAT au niveau des sites, générant une complexité échevelée.

A la fin des années 90, la plupart des grandes entreprises multinationales ont entrepris de vaste projet de rénovation de leur architecture réseau avec notamment l'adoption d'un plan d'adressage privé en classe A et la distribution des adresses par DHCP.

Fondamentaux du plan d'adressage

- Utiliser des adresses privées (RFC 1918 - 1996)
  - 24 bits block : 10.0.0.0 / 8 (=>10.255.255.255)
  - 20 bits block : 172.16.0.0 / 12 (=>176.31.255.255)
  - 16 bits block : 192.168.0.0 /16 (=>192.168.255.255)
- Planifier soigneusement en respectant hiérarchie / contiguïté
- Etablir un modèle de distribution par type de plage
- Attribuer les adresses automatiquement (DHCP)

Quelques adresses remarquables

0.0.0.0 désigne tout réseau. Route supportée par une gateway dans une table de routage
127.0.0.1 désigne l'instance courante de TCP (loopback)
224.0.0.0 – 239.255.255.255 adresses réservées pour le multicast

Hiérarchisation du plan d'adressage

Pourquoi hiérarchiser ?

Pour permettre un routage efficace en limitant la taille des tables de routage et en permettant une convergence rapide du réseau en cas d'ajout d'un site, de redémarrage, de modifications …

La hiérarchisation du plan d'adressage suppose l'usage d'un protocole de routage de type classless (RFC 1817) cad qu'on utilise un masque réseau dont le nombre de bit peut varier de 8 à 32 en continu.

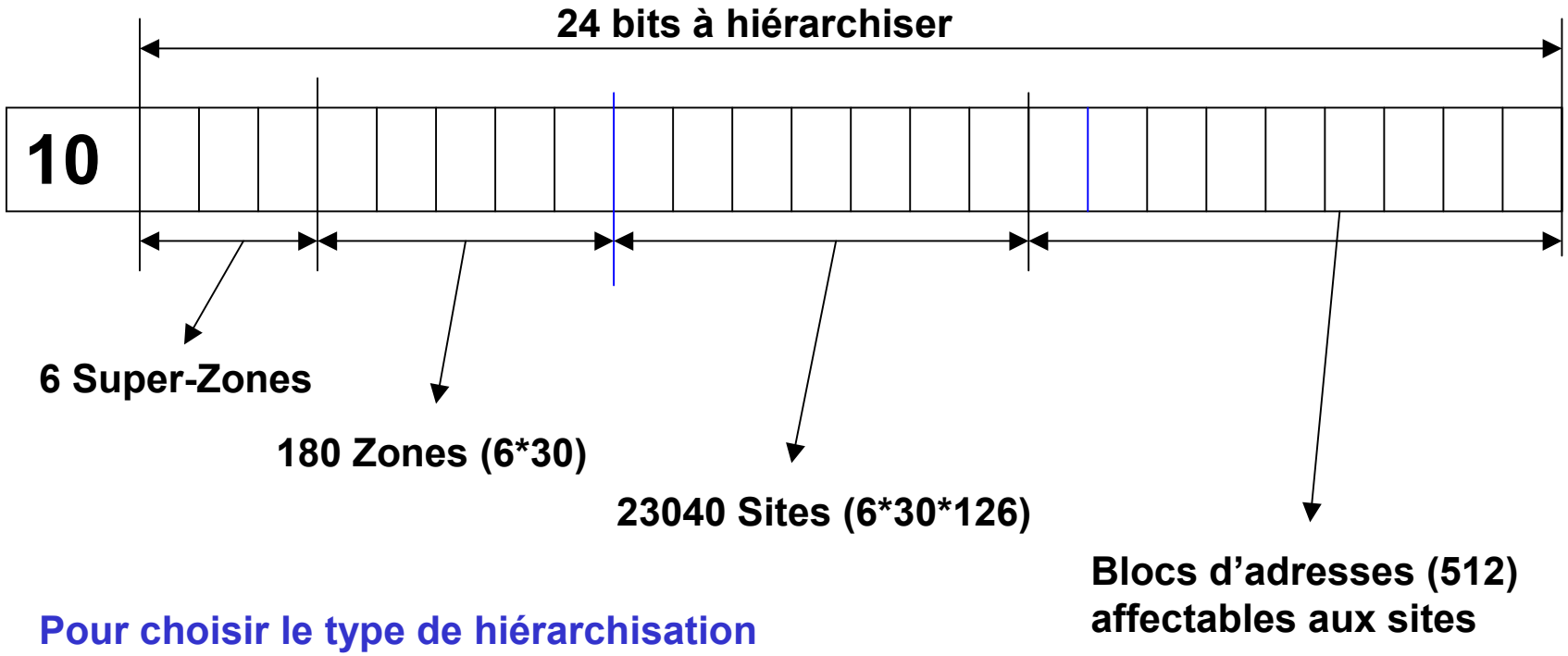
La hiérarchisation peut être appréhendée comme une mise en application du principe diviser pour régner (encore !) comme dans le réseau téléphonique ou chaque commutateur ne considère qu'une portion du numéro pour prendre une décision.

En considérant 2 positions décimales, la liste maximale de la table de commutation est 100, s'il fallait considérer les 10 postions décimales, la taille max serait de 10^10 !

La hiérarchisation permet aussi de définir les meilleurs endroits pour partager des ressources au niveau du réseau global (les accès internet, serveurs DNS par exemple)

Hiérarchisation du plan d'adressage

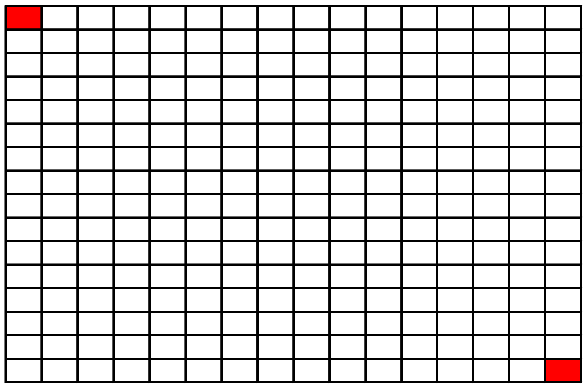
Exemple de hiérarchisation à 3 niveaux pour une multinationale



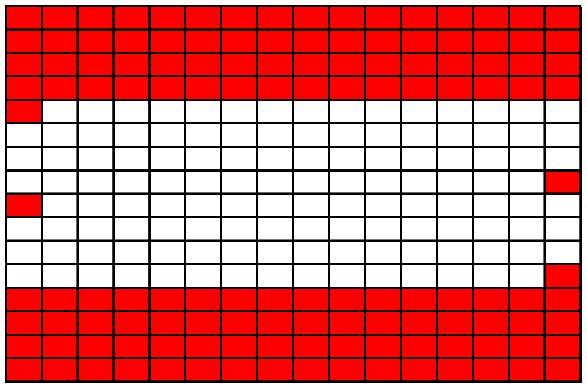
Pour choisir le type de hiérarchisation de votre PA, considérer l'implantation de l'entreprise sur une mappe monde à différentes époques.

Illustration de la perte d ’adresses induite par le subnetting. On suppose un espace de 8 bits

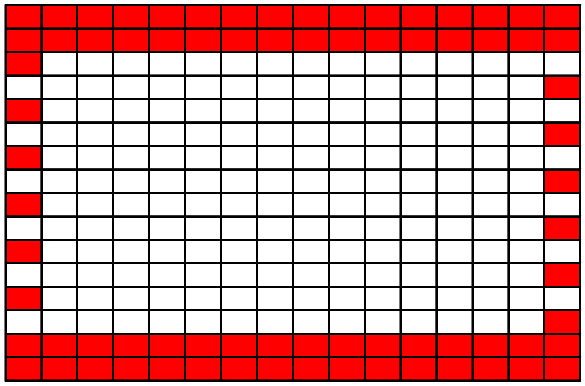
0 = 1 net - 254/256 adresses utiles



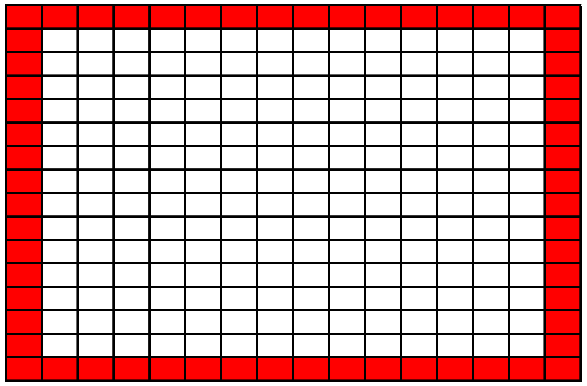
2 = 2 subnets - 124/256 adresses utiles



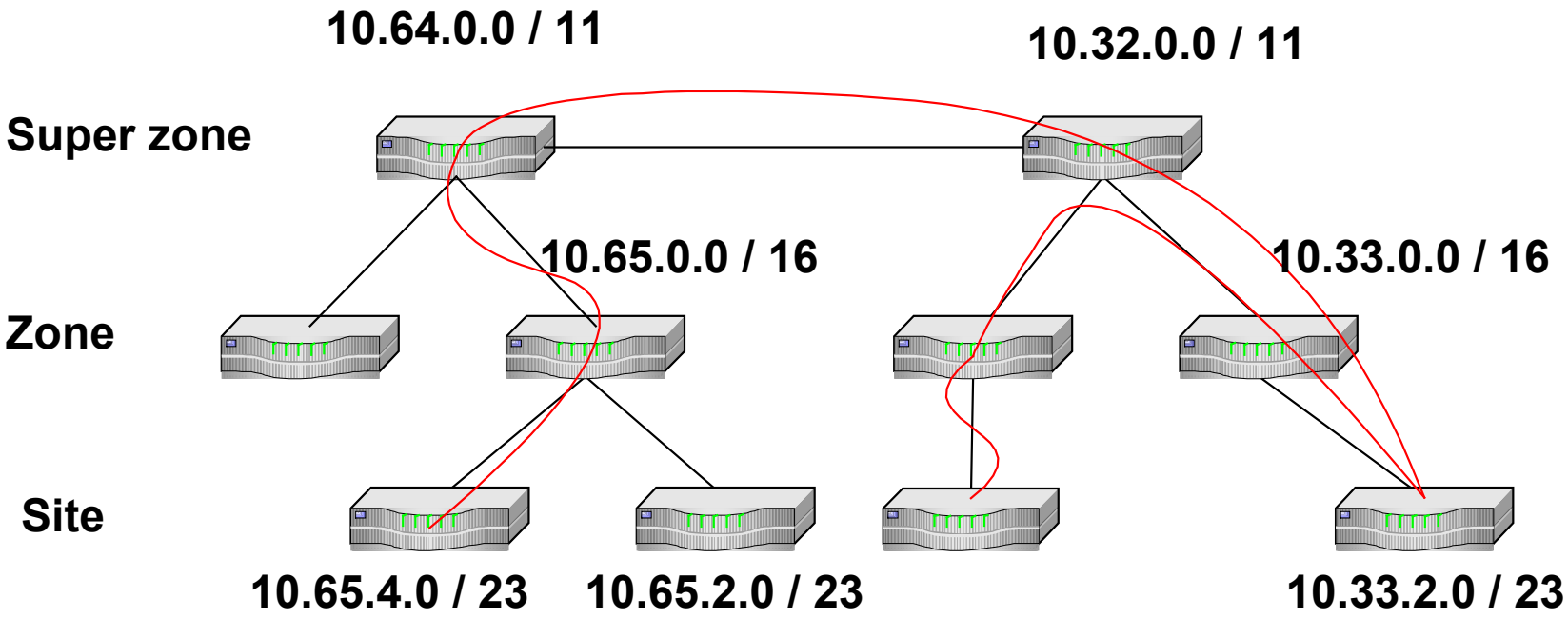
3 = 6 subnet - 180/256 adresses utiles



0 = 14 subnet - 196/256 adresses utiles



Hiérarchisation des routeurs



Les sites sont numérotés de droite à gauche :le site 10.33.1.0 représente le premier site de la première zone de la première super zone …

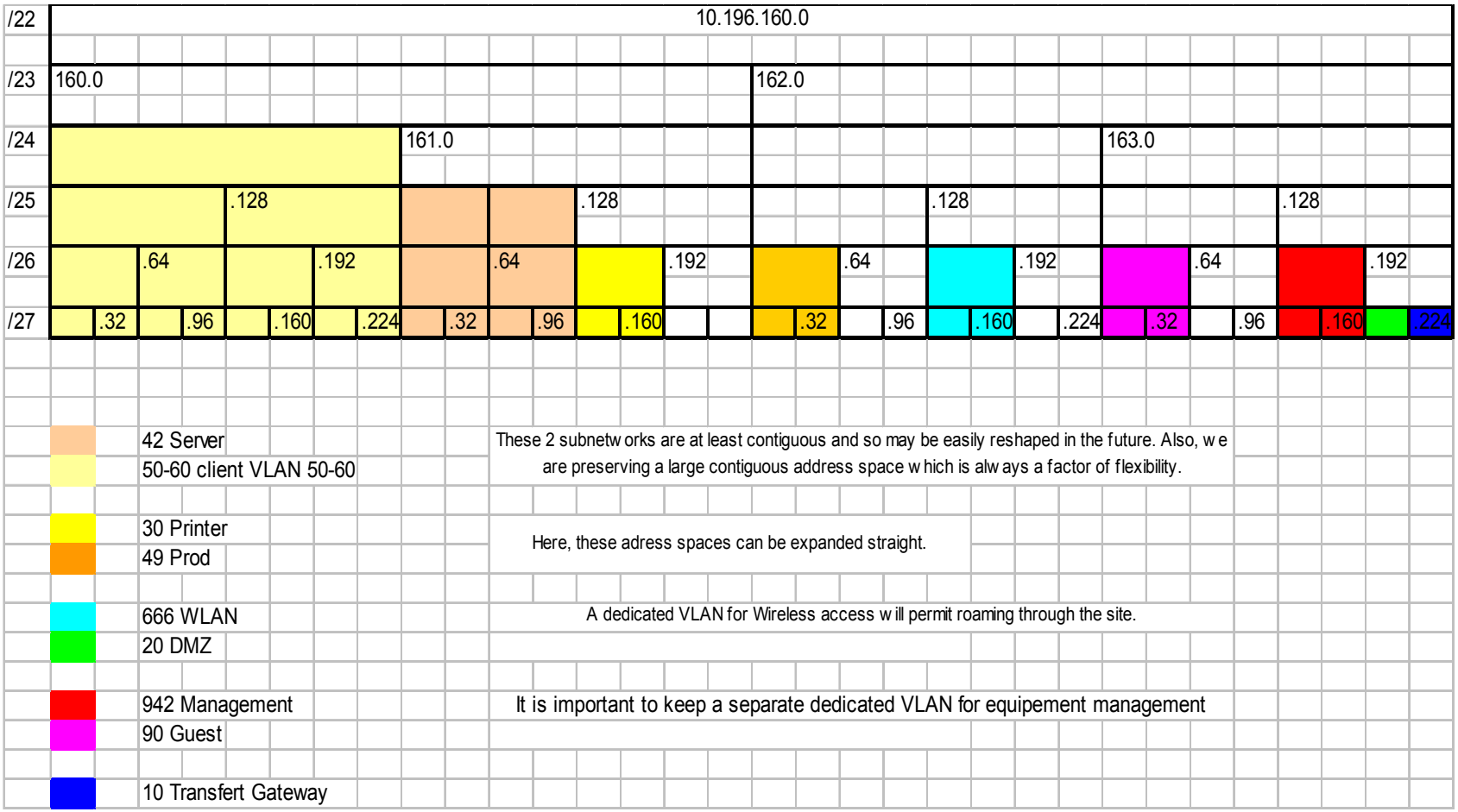
Modèles d'affectation d'adresses

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.

Modèles d'affectation d'adresses



Protocoles de routage (RP)

A quoi ça sert

Le meilleur moyen de comprendre l'utilité d'un protocole de routage et de ne pas en utiliser ! En fait la question ne pose plus. (Sauf si vous avez 3 routeurs à gérer).
Essentiellement un protocole de routage permet une adaptation automatique des routeurs aux modifications affectant le niveau 3 du réseau.

Notion d'Autonomous System AS

Pour une instance d'un protocole de routage donné sur un routeur correspond un identifiant. L'ensemble des routeurs interconnectés possédant le même identifiant définit un AS.

Un protocole de routage destiné à échanger des informations entre plusieurs AS est appelé ERP (Exterior Routing Protocol) par opposition à un IRP (Interior Routing Protocol) qui ne transmet d'information que dans son AS

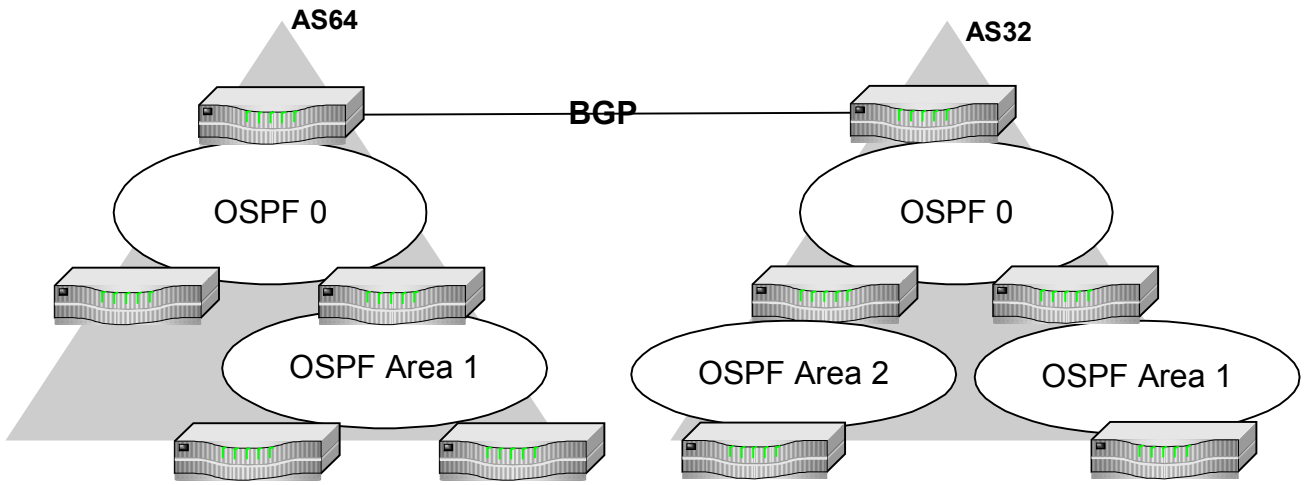
Quelques protocoles de routage de type IRP de type ERP

RIP V1 – IGRP	**OSPF (RFC 1583)**	
RIP V2 – EIGRP	**IS-IS (OSI**	**BGP**

Exemple d'utilisation des concepts de IRP ERP

Dans le fil de notre exemple de plan d'adressage hiérarchique, voici comment on pourrait structurer l'utilisation des protocoles routages.

- Chaque superzone est un AS
- On route entre les superzones avec BGP
- les routeurs de niveau intermédiaire de chaque SZ constituent le backbone OSPF (Area 0)
- les routeurs sites d'une zone donnée définissent une aire OSPF accrochée au backbone



La dynamique de l'offre WAN -1

On propose toujours des liaisons transfix 256 kb/s à 1500 € / mois pour 300 kms - plus frais de mise en service à chaque extrémité et les liaisons 2,4 et 4,8 kb/s ne sont plus commercialisées depuis mars 2005).

En fait le modèle de la ligne louée a perduré commercialement avec les technologies à commutation de paquets (ou de trames ou de cellules) alors qu'il y avait un écart de plus en plus grand entre la logique commerciale (fondée essentiellement sur le mix distance / débit point à point) et la réalité technique du réseau.

Parallèlement, les débits possibles ont littéralement explosés au cours des années 90. Grâce au multiplexage de longueur d'onde, d'après Pujolle (Les Réseaux - 2005) les débits sur fibre par exemple ont doublés tous les six mois entre 2000 et 2004, on atteint aujourd'hui plusieurs dizaine de Tbits/s !

L'offre commerciale de pointe depuis le début des années 2000 est une offre de niveau 3 / 4, fondée sur MPLS. C'est un service de VPN IP qui va jusqu'au routeur site. Les arguments commerciaux sont la souplesse et la sécurité en arguant que le réseau internet est évité. En fait ce dernier argument n'est-il pas la pour éviter au client de se dire que tout compte fait il peut faire la même chose sur internet et garantir sa sécurité avec un VPN ?

« *Le réseau IP MPLS de France Télécom repose sur un coeur de réseau comprenant 22 commutateurs haute capacité répartis sur 16 sites géographiques en France et 60 commutateurs à l'international. Il assure le transit de 192 Tera Octets par semaine en moyenne en France.* »
Notons que ceci représente 1536 Tb/s soit à peine 3 min sur un lien fibre 10 Tb/s

La dynamique de l'offre WAN - 2

La frontière de la partie sous-traitée en matière de WAN a tendance à empiéter de plus en plus profondément au sein de l'entreprise.

Historiquement, les entreprises disposaient des équipements réseaux et louaient des services de liaisons point à point entre ces équipements à des fournisseurs réseaux qui se chargeaient essentiellement d'assurer une continuité du signal et le transport des bits d'un équipement à l'autre.

Ce schéma, correspondant à celui de la ligne louée dédiée facturée à la distance et au débit, est largement obsolète.

La boite de pandore avait été ouverte avec l'arrivée de l'offre mutualisée des réseaux à commutation de paquets (TRANSPAC en France) qui connaît une longévité exceptionnelle (depuis 1978) et qui introduisait une facturation Débit/CV/Volume indépendante de la distance. Ensuite est arrivée l'offre Frame Relay profitant de l'augmentation de puissance des DTE et de la fiabilité accrue du transport. (FR abandonne la facturation au volume).

En fait depuis la fin des années 80, TRANSPAC par exemple achemine ses données sur FR, X25 subsiste seulement pour l'attachement terminal. Au cours de cette évolution, les opérateurs télécom ont du adapter leur métier aux couches supérieures du réseau. X25 comporte une couche 2 et une couche 3 par exemple et implique un routage initial pour ouvrir un CV.

Avec l'arrivée d'ATM, puis l'incroyable demande d'internet, les opérateurs télécom ont du entrer encore plus profondément dans le management de réseau en devenant des providers et ils ont définitivement du acquérir une culture de commutation de paquets alors qu'ils étaient historiquement sur des métiers de commutation de lignes.

La dynamique de l'offre WAN - 3

L'offre des opérateurs historiques de télécommunication a évolué d'une offre de circuit vers une offre de service clefs en main de niveau 3/4.

La réalisation technique de cette offre repose sur des technique de commutation FR ou ATM sous le protocole MPLS. L'infrastructure réseau est censée être séparée d'internet.

MPLS permet la mise en place de services telle VPN, CoS, VoIP. (En pratique et d'expérience la mise en œuvre des CoS est encore hésitante).

C'est une offre de sous traitance complète du WAN de l'entreprise jusqu'à la fourniture et la maintenance du routeur d'accès (CE : customer Equipment)

Cette offre est moins coûteuse et considérablement moins exigeante en ressources internes qu'une offre fondée sur des liaisons louées, elle devient pour cette raison incontournable pour la plupart des grandes d'entreprises.

Elle reste dans l'absolu très coûteuse si on la compare aux capacités de la technologie en matière de télécommunication et elle peut être mise en concurrence avec l'usage de VPN sur internet.

En pratique, ça ne se fait pas dans les grandes entreprises car d'une part cela nécessite une bonne expertise interne (et justement les entreprises se sont débarrassées de leurs experts au cours de la sous traitance aux opérateurs) et d'autre part il y a un sentiment d'insécurité qui paraît inacceptable pour le management.

En pratique cela ce fait de + en + dans les PME car la dimension des problèmes est moindre et nécessite donc moins d'expertise, ensuite les coûts sont plus déterminants, enfin ces entreprises ont souvent moins d'historique et donc moins d'à-priori.

Inventaire et documentation du niveau 3

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.

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)

Lors d'un déploiement vers un service WAN clef en main, voilà typiquement les informations qu'il faudra fournir pour couvrir le niveau 3

Inventaire des routeurs

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

Négocier son WAN - 1

Les degrés de liberté du client face au fournisseur sont assez faibles

Dans un pays donné, le marché reste souvent dominé par l'opérateur historique et ses filiales. (en France : FT Transpac, Equant, Oleane), donc faire jouer la concurrence est encore rarement une option.
C'est surtout la taille qui sera prépondérante, si vous êtes encore petit, faites miroiter des acquisitions !

Que va-t-on négocier ?

- **Etendue et limite du service : en général un routeur du fournisseur sur le site**
- **Gestion des liaisons de backup ISDN**
- **Gestion de la ligne de télémaintenance RTC**
- **Accès internet (qui gère la sécurité ?)**
- **Accès Nomade (qui gère l'authentification ? Coût des changements ?)**
- **Nombre de VPN**
- **Coût des opérations de gestion basiques : mise en service d'un site, déplacement d'un site, ajout ultérieur d'un site, suppression d'un site.**
- **définition des classes de service et coût associé**
- **Définition des SLA autour des paramètres techniques : débit délai, gigue, taux de perte**
- **Définition des SLA autour des paramètres de service : helpdesk, ouverture de ticket, délai de remise en service, mesures réseaux et condition d'accès**

Négocier son WAN - 2

Le cas des CoS

L'opérateur peut proposer des CoS standards ou des CoS spécifiques au client peuvent être négociées.
Une bonne utilisation des CoS nécessite de bien connaître les flux de son réseau, si on n'est incapable de les qualifier, il est parfaitement inutile de négocier des CoS.
Cela n'empêche pas de le faire ultérieurement mais alors, cette possibilité doit être prévue au départ du contrat pour ne pas risquer de mauvaises surprises.
Il y a aussi d'autres problèmes à gérer avec les CoS : si tous les sites n'ont pas le même niveau, que se passe-t-il lorsqu'un site ayant un CoS donné dialogue avec un site d'un CoS de niveau différent ? Les réponses peuvent varier en fonction des protocoles.

Le plan d'adressage

Vérifier la compatibilité de votre plan d'adressage actuel avec l'offre, ceci ne fait pas partie de la négociation commerciale à proprement parler mais il est bon de l'évoquer le plus tôt possible pour des questions de charges internes et de planning.
Typiquement, s'il n'est pas sur une classe d'adresses privées, il y a de grandes chances pour que vous deviez re-numéroter !
De même un plan d'adressage hiérarchique sera largement préférable pour des raisons de performance puis de diagnostic, de fiabilité, rapidité de convergence … ce n'est pas parce que votre réseau est sous-traité que ces problèmes disparaissent !

Déployer son WAN - 1

Une fois les conditions techniques négociées, accord et signature définitifs interviennent dans les 3 mois. (je suis peut être mauvaise langue !)

Vous allez alors passer en mode projet avec votre fournisseur

Vous devez vous rendre compte que votre fournisseur est en fait toujours en mode projet, donc il n'est jamais en mode projet ! Il n'a pas qu'un client, et les équipes de déploiement son les mêmes pour tout le monde.

L'inconvénient est le suivant : il sera difficile de négocier une méthode spécifique, le fournisseur vous imposera ses documents, sa présentation des données …
Ceci dit, il y a toujours une opportunité de négocier cela au tout début à condition que vous soyez capable de proposer tout de suite un mode de présentation existant qui garantit la disponibilité des données nécessaires au déploiement.

C'est à ce moment que vous comprendrez l'utilité d'une bonne documentation de votre réseau car si vous vous montrez hésitant et peu sûr de ce que vous êtes capable de fournir à ce moment là, le fournisseur imposera sa méthode et vous devrez vous y plier. Si vous n'aviez rien, c'est le moindre mal, mais rallongera considérablement les délais de mise en œuvre, si vous aviez déjà une information structurée, vous devrez en gros la dupliquer sous une autre présentation, ce qui n'est jamais agréable.

Les informations nécessaires :

Votre plan d'adressage
Les « fiches de sites »

Déployer son WAN - 2

Mise en place de la trame projet – étapes d'initiation

Constitution d'une équipe projet, des règles de sécurité, de la classification des informations (confidentialité), structure de circulation de l'information.
Validation du plan d'adressage
Définition des zones de déploiement (dont infrastructure)
Désignation d'un responsable de zone
Définition d'un rythme de déploiement par zone
Mise en place interface ancien réseau / nouveau réseau (équipe réseau centrale)
Recueil des informations par site
Préparation des serveurs DHCP et DNS avec les nouveaux paramètres (s'il s'agit de nouveaux serveurs, on voit qu'il faut s'y prendre tôt)

Les étapes basiques du côté client

Mise en conformité et validation
Commande / affectation des lignes de backup
Commande / affectation des lignes de télé-maintenance
Transmission des fiches de sites
Planification de la livraison du routeur
planification de la résiliation de l'ancienne ligne
Livraison / raccordement des routeurs
Validation de la ligne de télé-maintenance
Planification de la mise en service
Mise en service.
Tests niveau 3 : connectivité avec l'ancien réseau et le nouveau réseau
Test backup, Test synchro horaire, Tests spécifiques (DHCP …)

Déployer son WAN - 3

Voilà ! Nous avons un nouveau routeur sur le site

Une fois le routeur mis en service sur le site, le fournisseur considère que son service est facturable si rien de particulier n'a été négocié à ce sujet.

Pour le client il s'agit maintenant de faire basculer son trafic réseau vers ce nouveau routeur et souvent c'est là que le plus gros du travail commence.

Basculer vers le nouveau réseau

En général il y a une période de recouvrement où les 2 accès vont subsister côte à côte. Cette période définit le délai disponible pour effectuer la bascule, dépasser ce délai peut être grave en terme de rupture de service et /ou de coût. Il peut aussi se produire dans ces périodes des arrêts intempestifs de contrats. Il vaut mieux faire au plus tôt.

L'outil de base pour la bascule : DHCP DNS

En général, les clients acquiert l'indication de leur Gateway par DHCP (s'ils n'en ont pas, ils utilisent ARP, ou un protocole de découverte de routeur : IGDP)
On voit que si ce point n'est pas connu à l'avance, on a peut être déjà des clients qui se sont basculés tout seul !

Les informations fournies au client par DHCP : @IP, mask, GW, DNS, NTP, domain suffix, éventuellement : SLP (encore rare), WINS dans l'univers Microsoft (encore trop courant)

On réalise que nous entrons dans le niveau 4 !

Exploiter son WAN -1

Passage en mode exploitation

Une fois le projet de déploiement terminé, vous allez passer en mode exploitation avec votre fournisseur. Le même problème va se poser, qu'au moment de passer en mode projet : vous vous apercevrez que votre fournisseur ne distingue définitivement pas le mode projet du mode exploitation.
Par exemple, lors du déploiement, vous avez du spécifier un nom de contact local, qui était une personne adaptée de votre point de vue au mode projet.
Maintenant, vous souhaiteriez voir un autre nom à la place, celui d'une personne concernée par l'exploitation quotidienne. C'est un premier bon test !

Rodage de la gestion des incidents

En général, et le fournisseur en est assez fier, il y a un numéro de téléphone unique (pudiquement helpdesk) pour lequel vous avez dû faire agréer une liste de noms. En cas d'incident vous appelez et le helpdesk ouvre un ticket.
Vous pourrez éventuellement vous rendre compte que le helpdesk n'a pas les mêmes références que vous. Par exemple des références sites avaient été affectées et vous les avez consciencieusement notés dans votre documentation.
Le helpdesk ne semble pas les connaître et vous demande l'adresse IP du routeur, comme vous avez diffusé une procédure au personnel décrivant le mode d'ouverture d'un ticket précisant d'utiliser le n° de site, il y a du flottement.
En fait, trop souvent (jamais vu autrement en fait) le helpdesk ne sert qu'à protéger l'opérateur de l'intrusion de ses clients et ne fait que gérer administrativement un incident pour satisfaire au cahier des charges et fournir les statistiques qu'il vous sera très difficile de contrôler et de contester (en fait le helpdesk peut ouvrir aussi des incidents dont vous n'aurez jamais connaissance)

Exploiter son WAN - 2

Donner un rôle d'interface utile au helpdesk

On s'aperçoit vite que le helpdesk est incapable de vous fournir le moindre renseignement utile sur l'état de traitement de l'incident en terme de :

-Diagnostic
-Etendue des perturbations (sites concernés nature des perturbations)
-Délai vraisemblable de remise en service à 50 % 80 % 100 %
Souvent aussi, des choix doivent être fait qui vont privilégier tel groupe de sites par rapport à tel autre au cours du traitement de l'incident.
Ces décisions ne devraient pas être prise sans consultation du business qui peut donner par exemple des plages acceptables de coupure ou de dégradation de tel ou tel service sur tel groupe de sites etc …
Ce travail d'interface entre les nécessités techniques et les souplesses/rigidité du business devrait être le rôle typique du helpdesk qui verrait sa valeur ajouté monter ainsi que son efficacité en prenant un peu de connaissance sur les souplesses permises par l'activité.

Analyse post mortem

Il est bon de se réserver, avant la signature, le droit de réclamer auprès de votre fournisseur l'analyse exhaustive et minutieuse d'un certain nombre d'incidents par période de temps (2 par trimestre par exemple). Cela signifie que pour le ticket xyz, votre fournisseur doit être en mesure de vous communiquer un historique exact de toutes les opérations associées au traitement, liste des communications, mail, téléphones, date, heure, identification des interlocuteurs … Je peux vous garantir que c'est instructif !

Niveau 4 : services réseaux fondamentaux

Objets Physiques	Objets Logiques	Concepts	Anticipation / Pérennité
Serveurs Infrastructure	DHCP DNS SLP NTP NDS AD LDAP ZenWorks SMS SMTP POP IMAP SNMP	Gestion de noms Authentification Représentation des objets du réseau Messagerie	1 - 3 ans Stratégique / 5-15 ans / historique

On ne conçoit pas un réseau TCP sans les services DHCP et DNS, ils constituent les services basiques minimaux de cet environnement.

La nature de ces services doit être clairement comprise par l'entreprise, ils doivent être dominés et documentés.

Sur ces services de bases on trouvera de plus en plus souvent un service d'annuaire, auquel cas la synchronisation horaire du réseau sera un impératif (elle est de toute façon vigoureusement conseillée)

DHCP DNS
Gestion de la frontière (NAT / DNS)
Annuaire d'entreprise

DHCP DNS : documentation - questions

A documenter : DHCP

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

A documenter : 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, redirecteurs …)
Comportement des clients (requêteurs)

Questions

Nombre des serveur DHCP ? DNS ? Ou les placer ?
La réponse est dans le design niveau 3.
Le client accède à un serveur DHCP par broadcast, comment traverser les routeurs ?

Gestion de la frontière

NAT

L'utilisation d'un espace d'adresse privé implique l'usage de NAT pour communiquer avec l'extérieur.

NAT est exécuté en général sur un firewall qui supporte en même temps des services proxy (qui eux aussi font du NAT).
Network Address Translation : en fait ne traduit rien du tout, il substitue à une adresse d'émission privée qui ne signifie rien, une adresse publique, routable sur internet, jusque là c'est simple, c'est lorsque les paquets reviennent que l'affaire se complique …
NAT peut intervenir dans un autre cas de frontière : l'usage des classes d'adresses privées s'est répandue, 2 compagnies doivent fusionner, ou simplement elles doivent établir une liaison pour leurs affaires, si elles sont toutes les 2 sur la même classe d'adresses, il y un problème, que NAT peut permettre de résoudre à court terme. (à moyen terme, dans le cas de la fusion, il est peut être préférable de fusionner les plans d'adressage en re-numérotant la où c'est nécessaire).

Les protocoles qui ne sont pas copains avec NAT :

Ceux qui transfèrent des adresses IP au sein du paquet de donnée … (FTP)
ceux qui utilisent le checksum fondé sur l'adresse originale, bien que NAT le recalcule, celui d'origine a pu être utilisé pour crypter quelque chose dans la zone data …

Gestion de la frontière DNS

Identités DNS

Dans la foulée de l'utilisation d'un espace d'adresses privées, vous avez tout intérêt à utiliser un espace de nom de domaine privé distinct de celui par lequel on vous connaît sur internet. (Internet : tranchedebrie.com / local : tranchedebrie.local)

Votre structure DNS interne gérera votre espace de nom privé sous .local et vos postes de travail pointeront sur vos DNS internes. Jusque là tout est simple. Les questions et les choix à envisager interviennent lorsqu'un utilisateur veut résoudre un nom DNS hors de votre domaine (.com par exemple).

Traitement des requêtes hors domaine par le DNS interne

Identifiant que le domaine ne le concerne pas, le serveur a 2 façons de réagir suivant que la requête est récursive ou non (=> choix de réglage de la station de travail)
- prendre un serveur dans la liste des root pour et en renvoyer l'adresse à la station
- Interroger lui même le root et suivre le fil des réponses jusqu'à trouver et répondre à la station

Implications

Dans le premier cas, les stations devront émettre des requêtes DNS vers internet et il faudra faire en sorte que la réponse puisse passer à travers le(s) firewall, en général ce n'est pas une solution que l'équipe sécurité voit avec enthousiasme.
Dans le deuxième cas le problème est similaire mais limité aux serveurs DNS et les règles à emplanter sont raisonnables.
Enfin on peut utiliser un proxy DNS sur un firewall (dans ce cas les 2 options ci-dessus restent ouvertes !

Annuaire d'entreprise -1

Un annuaire d'entreprise est une base de données dont l'accès doit être assuré en tout point du réseau de l'entreprise et qui contient les objets représentant des unités de gestion plus ou moins sophistiqués du système d'information.

L'annuaire est typiquement organisé de façon arborescente au sein d'objet de type conteneur (Country, Organisation, Organisation Unit). Cette organisation est associée à une convention de nommage des objets issue historiquement de X500.

Les objets que l'on peut représenter sont : utilisateurs, groupe, poste de travail, serveurs, imprimantes, serveur d'imprimantes, queues, listes de distribution, serveur de messagerie, package applicatifs, …
éventuellement des objets plus techniques : scope DHCP, zone DNS, directory SLP, …

En fait les objets représentables sont définis dans un schéma qui peut être étendu par API.

L'annuaire d'entreprise donne ainsi un point unique de gestion des objets gérés par l'administration réseau.

Il donne un point d'entrée unique pour la gestion des utilisateurs, des postes, des permissions, de la distribution de logiciel.

Il est le seul support administrativement envisageable pour la gestion contrôlée des clefs publiques/privées permettant de fonder les bases de l'ID management.

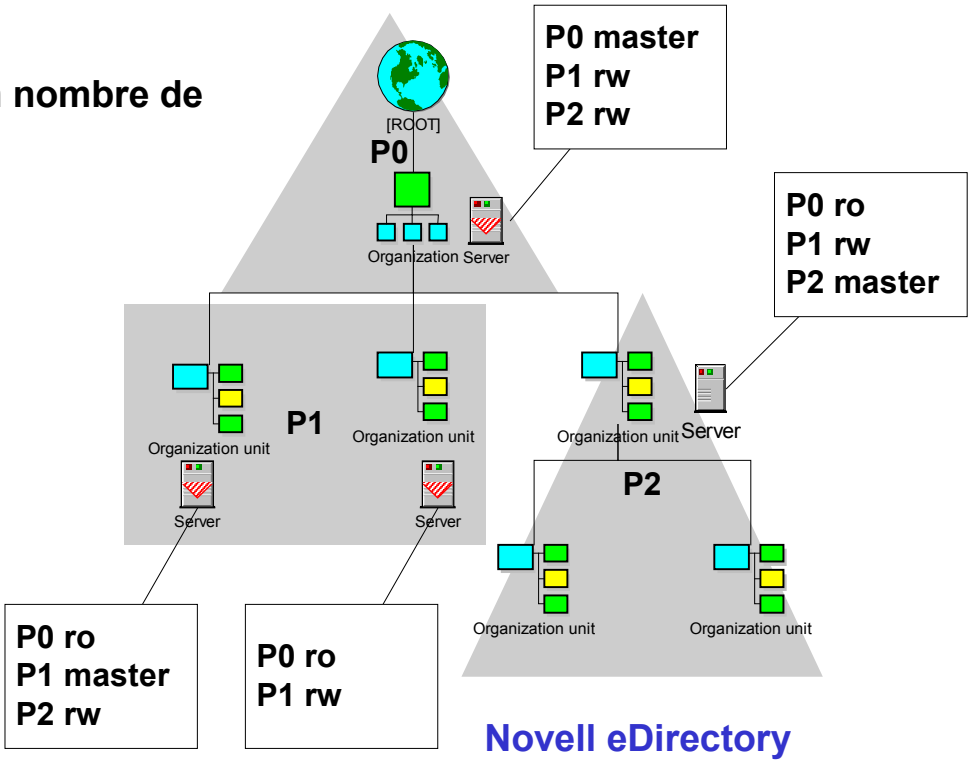
Annuaire d'entreprise - 2

Ce schéma montre une arborescence composée d'une organisation et un certain nombre de sous-organisations.

Les zones grisées correspondent à des partitions.

Les serveurs supportent un certain nombre de replicas de ces partitions.

L'annuaire d'entreprise est un des concepts les plus ambitieux et les plus riches de promesses pour le management efficace des SI modernes. Il n'est pourtant pas encore vraiment passé dans la culture des administrateurs, 15 ans après la sortie de NetWare 4 et de NDS !



Novell eDirectory supporte des annuaires de plusieurs dizaine de millions d'objets lourds.

Supervision : vue classique des tâches

Tâches organisation / administration

Inventaire matériel
Inventaire logiciel
Inventaire utilisateur
Inventaire données / répertoires
Inventaire gestion des droits d'accès aux données / logiciels / imprimantes

Tâches issues du système

Fonctionnement des process
Charges CPU / mémoire
Occupation disques
Sauvegardes
Impressions

Tâches issues du réseau

Surveillance
Gestion des incidents
Analyse de trafic (charge / temps, contenu)

Tâches 'modernes'

Messagerie
Antivirus

A partir d'une liste de ce type on rêve d'une console qui centralise le tout et permet de changer un droit par ci, de distribuer un logiciel par là, d'éditer une liste de stations par site …

Ce point de vue est trompeur.

Supervision : point sur SNMP

Depuis la fin des années 80, SNMP s'est imposé comme le standard de fait pour le 'management' d'objets physiques et logiques accessibles par TCP.

SNMP définit

La distinction système de management / système managé
Un protocole de dialogue entre les 2 types de systèmes

Get ([request] [next-request]), Set (Request de Management vers Managé
Get (response), Trap de Managé vers Management

SNMP implique une couche cliente sur chaque élément à manager.
L'accès en lecture / écriture est contrôlé par une simple chaîne de caractères spécifiée au niveau du client.

La structure des messages est décrite par les MIB

La structure des réponses est défini dans ce qu'on appelle les MIB (management Information Base) qui ne sont pas du tout des bases de données mais une liste de switchs, de compteurs, de variables, suite d'octets … correspondant à certaines caractéristiques spécifiques à l'objet managé.

Il y a 2 niveaux de MIB : SNMP MIB original et MIB 2 qui comprend 165 objets.
Maintenant, chaque constructeur / éditeur va ajouter 150 / 200 MIB personnels.
Les outils de management utilisent une représentation interne des MIB qui leur est propre et pour cela 'compilent' les MIBs présentées au format texte avant de pouvoir les utiliser.

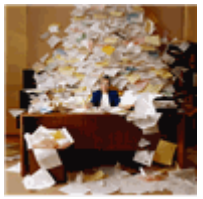
Supervision de grands systèmes : philosophies - 1

Mise en évidence d'un comportement hors norme

Le système de surveillance interroge l'état d'un équipement (ou du moins il essaye). Lorsqu'un état du système mesuré est arrivé à une certaine valeur jugée en dehors de normes pré-établies, il enregistre un événement. Un tel système n'enregistre rien concernant le fonctionnement normal du système surveillé.
Ces systèmes classiques mettent typiquement en évidence l'équipement concerné par une alerte de haut niveau en rouge sur une représentation graphique à l'écran, jusqu'à ce que l'opérateur l'ait acquittée.
C'est un principe fondé sur l'exception. Si l'alerte devient le cas général le système de surveillance ne peut plus fonctionner.

Analyse de performance

A l'inverse du système précédent, le système va cette fois enregistrer un certain nombre de données choisies parmi les activités du système surveillé. Ceci afin de dégager des tendances et des rapports périodiques. A noter que les données enregistrées peuvent vite représenter des volumes très importants.
20 variables toutes les 5 minutes pour 100 équipements = 576 000 échantillons / jour * 64 octets / échantillons = 36 Mo / jours = 1 Go / mois. Pour 1000 équipements = 10 Go. Ce n'est tout de même pas négligeable.
Il faut penser que toutes ces informations sont collectées localement dans une BD et qu'on les consolide en un seul point. Pour un grand réseau ces systèmes trouvent leur limite dans les volumes de données à consolider sur une BdD centrale à partir de BdD réparties sur le WAN.



Supervision de grands systèmes : philosophies - 2

Les 2 systèmes ci-dessus ont une histoire divergente

Ce sont des fournisseurs distincts avec des environnements de développement, structure de données, interface, API … totalement différents qui n'ont aucune chance de se rejoindre dans une quelconque intégration et qui nécessitent des experts propres à chaque type d'outil pour la mise en œuvre à grande échelle.

Analyse agrégée

Réalisant que les volumes énormes de données n'étaient pas vraiment gérables (très vite les données collectées dépassent les capacités de traitement, d'interprétation humaine …) l'idée d'agréger les données au fil de l'eau a été mise en pratique à travers notamment un best no-seller : le freeware MRTG (Multi Router Trafic Grapher) apparu en 1994.

L'agrégation centrale ne passe pas l'échelle

Par ailleurs, on semble renoncer maintenant plus raisonnablement à agréger les données dans une base de données centrale. L'application va elle même chercher ce dont elle a besoin dans les diverses bases locales. Cela rajoute de la complexité au niveau de l'application mais c'est la seule alternative pour se débarrasser du goulet d'étranglement et de la consommation en bande passante (à travers un WAN !) que représente la BdD centrale (le plus souvent sur un serveur haut de gamme !)

En clair, les systèmes de type analyse de performance lacked scalability !

Vue prospective sur la supervision

Diviser pour régner (encore !)

Gérer les couches basses du réseau (2/3) à part de l'administration.

Définir des OU qui correspondent à des unités de gestion et de supervision logique.

Définir des points de collectes d'information au niveau de ces OU (au plus près de la source d'information – au niveau du site).

Ces points de collectes doivent être sur un annuaire répartie partitionné de façon à en permettre un accès aisé à partir de n'importe quel point du réseau (sans surcharger le LAN).

Ces points de collectes peuvent autant que possible être représentés comme des objets dans l'annuaire.

Gérer par événement et changement d'états au fil de l'eau plutôt que reconstituer par vague périodique.

C'est au moment d'un événement sur un objet qu'on dispose de l'information et c'est à ce moment qu'on doit la conserver, si la modification s'effectue via l'accès à la représentation de l'objet dans l'annuaire, il n'y a pas d'action spécifique à ajouter pour en garder trace.

Le point faible de la supervision actuelle est qu'on reconstitue l'état des objets en les scrutant un à un au lieu de garder trace des modifications et donc de bénéficier de la connaissance de l'état n-1. C'est la différence entre transmettre 24 images complètes par seconde ou 1 images puis les 24 modifications cumulatives.