Chapitre 11

Études de cas

Ce chapitre donne un aperçu des problèmes d'installation d'un réseau au moyen d'études de cas, depuis un petit réseau domestique jusqu'à des réseaux installés chez les *grands comptes* (grosses entreprises possédant de nombreux équipements interconnectés). Avec l'usage croissant des réseaux et le renouvellement rapide des matériels, il nous a paru opportun de proposer, dans un chapitre à part, des exercices qui fassent appel à des notions réparties dans plusieurs chapitres.

Cas 1 : Un petit réseau sans fil à la maison

Énoncé

Vous aviez connecté plusieurs ordinateurs à la maison (voir chapitre 5, exercice 1 et chapitre 10) par une liaison sans fil. Vous décidez de vous abonner auprès d'un opérateur qui offre, moyennant un forfait mensuel, une liaison ADSL à haut débit ainsi qu'une utilisation illimitée de votre téléphone vers des postes fixes situés dans toute la France. Pour cela, on vous a fourni une *zbox*, que vous devez configurer pour votre accès Internet et brancher sur une prise téléphonique. Cet équipement vous permet de créer votre réseau local, soit filaire par Ethernet, soit sans fil par Wi-Fi (802.11g). En installant votre *zbox*, vous constatez que, pour bénéficier de la gratuité des communications téléphoniques, vous devez brancher votre téléphone directement sur la *zbox* et non sur une prise de téléphone.

a Disposez-vous d'un service téléphonique classique ou de téléphonie sur IP (*ToIP*) ?

b Pour utiliser le réseau sans fil, vous avez une clé WEP de 26 caractères alphanumériques et vous devez définir le SSID du réseau ainsi que les adresses MAC des machines à connecter. Pourquoi ces précautions sont-elles insuffisantes pour protéger votre réseau sans fil contre des intrus malveillants ?

La *zbox* vous permet de partager l'accès ADSL entre les ordinateurs de votre réseau local, connectés soit par Ethernet, soit par Wi-Fi (voir tableau 11.1). L'adresse IP de la *zbox* est `192.68.1.1`. Votre réseau local est constitué de quatre ordinateurs et d'une imprimante, raccordés de la manière suivante :

Tableau 11.1

Types d'accès des différentes machines à connecter

Machine	Type d'accès au LAN
Ordi_1	Ethernet
Ordi_2	Ethernet
Imprimante	Ethernet *ou* Wi-Fi
Ordi_3	Wi-Fi
Ordi_4	Ethernet *et* Wi-Fi

c Combien consommez-vous d'adresses IP pour l'ensemble des équipements à connecter (autres que la *zbox*) ?

d Proposez les adresses IP que vous affecteriez aux différents équipements.

e L'adresse IP de la *zbox* est une adresse IP de réseau privé (définie par la RFC 1918). Beaucoup de *zbox* possèdent donc cette même adresse ! Comment est-ce compatible avec la notion d'unicité des adresses IP ?

Solution

a De *ToIP*, puisque c'est sur la *zbox* elle-même que le téléphone est branché. Sinon, il aurait fallu mettre un filtre sur la prise utilisée pour le téléphone.

b Car ces précautions standard sont des précautions statiques : les clés peuvent être largement diffusées, et on peut fabriquer une adresse MAC sur mesure (les outils de configuration donnent les adresses MAC en clair…). Une précaution possible serait de masquer la bannière du réseau (diffusion permanente du SSID) afin que le réseau sans fil ne soit pas directement visible par une personne se promenant dans la rue.

c Il faut 6 adresses IP en tout : trois pour les ordinateurs 1 à 3, une pour l'imprimante (elle ne fonctionne que dans un seul mode à la fois) et deux pour l'ordinateur 4.

d Puisque l'adresse attribuée à la *zbox* est une adresse privée (voir la RFC 1918), construite à partir de l'adresse réseau `192.168.1.0`, vous pouvez utiliser pour vos machines les adresses IP allant de `192.168.1.2` à `192.168.1.7`. Le tableau 11.2 donne un exemple d'affectation des adresses IP de votre réseau.

Tableau 11.2

Affectation des adresses IP aux machines de votre réseau

Machine	Adresse IP
Ordi_1	192.68.1.2
Ordi_2	192.68.1.3
Imprimante	192.68.1.4
Ordi_3	192.68.1.5
Ordi_4	192.68.1.6 & 192.68.1.7

e L'adresse IP étant une adresse privée, elle n'est valable qu'à l'intérieur du réseau considéré (c'est une adresse ambiguë, non routable). Pour pouvoir naviguer sur Internet, votre fournisseur d'accès à Internet (FAI, ISP – *Internet Service Provider*) a attribué à votre *zbox* une adresse IP routable, parmi toutes celles qui lui ont été attribuées par l'IANA (le FAI fournit en général une seule adresse IP routable par accès ADSL). Un DHCP partage l'accès à Internet entre toutes les machines de la maison et leur octroie des adresses privées comme celles du tableau 11.2. Vous pouvez aussi allouer manuellement à vos machines les différentes adresses IP. Cette dernière solution se révèle indispensable lorsque l'un de vos équipements ne fonctionne en réseau qu'avec une adresse IP prédéterminée.

Cas 2 : Architecture d'un réseau sans fil plus étendu

Énoncé

Une entreprise vous demande d'installer un réseau sans fil entre les bureaux et les salles de réunion du siège social, lequel est réparti entre deux bâtiments proches l'un de l'autre. Le futur WLAN doit être compatible avec le réseau Ethernet filaire de l'entreprise.

a Quelles options s'offrent à vous ?

b Proposez une solution pour installer ce nouveau réseau sans fil dans un premier bâtiment.

c De quels matériels avez-vous besoin ?

d Quelles précautions devez-vous prendre pour relier vos différentes bases ?

e Vous décidez de relier le second bâtiment par le WLAN. Quelles sont les conséquences de cette extension ?

f Décrivez les étapes à respecter pour configurer votre WLAN.

g Vous souhaitez doter le WLAN d'un minimum de sécurité. Quelles précautions envisagez-vous ?

Solution

a Vous commencez par vous documenter sur les réseaux sans fil. Plusieurs standards coexistent : 802.11a, 802.11b et 802.11g. Les deux premiers sont incompatibles entre eux ; le dernier offre le même débit que 802.11a tout en étant compatible avec le standard 802.11b.

b Vous décidez donc d'acquérir des matériels certifiés Wi-Fi[1], supportant le standard 802.11f[2], de façon à installer votre WLAN à partir d'équipements de différents constructeurs. Vous choisissez le standard 802.11g, qui vous offre des débits allant jusqu'à 54 Mbit/s, sans les contraintes strictes imposées aux WLAN fonctionnant en 802.11a. Votre réseau sera un réseau *à infrastructure*, vous permettant d'installer suffisamment de bornes d'accès pour bien desservir l'ensemble du bâtiment.

c Au minimum, il vous faut une base (on parle également de *borne* ou de *point d'accès*) et autant de cartes Wi-Fi que d'ordinateurs portables souhaitant utiliser le WLAN. La base doit posséder la fonction de pont, pour qu'on puisse la raccorder au réseau Ethernet filaire de l'entreprise. En outre, vous devez acheter des antennes de différents types, selon l'utilisation qui en sera faite et le type de local à raccorder. Le tableau 11.3 récapitule les différents types d'antennes et l'usage auquel elles sont destinées.

Tableau 11.3

Les différents types d'antennes pour réseaux sans fil

Type	Locaux à desservir
Verticale	Salles de réunion, bureaux
Dipôle	Couloirs (zones étroites et longues)
Sectorielle	Salles de réunion ou halls d'entrée
Yagi	Liaison entre bâtiments proches
Parabolique	Liaison entre immeubles éloignés

d Les différentes bornes d'un WLAN étendu doivent se situer dans le même domaine de collision et appartenir au même sous-réseau IP, pour que vos utilisateurs puissent se déplacer dans tout le bâtiment sans perdre la connexion au réseau (pour cela, vous avez choisi des matériels compatibles supportant le standard 802.11f).

Pour desservir tout l'immeuble, vous devez placer vos bornes de sorte que leurs zones de couverture se chevauchent. Pour connaître le nombre de bases nécessaires, vous pouvez utiliser des outils qui simulent votre futur réseau. Plus simplement, vous vérifiez votre installation en vous promenant avec un ordinateur portable (doté d'un logiciel de test affichant la puissance du signal reçu). Vous vous assurez ainsi qu'il n'y a pas de zones d'ombre et que la puissance du signal reçu est suffisante dans toutes les zones[3].

e Deux possibilités s'offrent à vous, selon la distance entre les deux bâtiments : soit vous augmentez la portée du WLAN en exploitant le mode répéteur de certaines bornes, à l'aide d'antennes de type *parabolique* ou *yagi*, soit vous installez dans l'autre bâtiment de nouvelles bornes, raccordées comme les autres par un Ethernet filaire et obéissant aux mêmes conditions d'appartenance (même domaine de collision et même sous-réseau IP).

Avec la mise en cascade de certaines bornes en mode répéteur, vous divisez le débit utile par deux, puisque les bornes se partagent le même canal pour communiquer entre elles et avec les stations (la borne faisant office de répéteur transmet la trame à l'autre borne avec la même fréquence). Cette solution ne sera pas retenue si vous souhaitez disposer du débit le plus élevé possible. Dans ce cas, les contraintes d'appartenance peuvent être délicates à respecter selon la topologie des lieux.

f La configuration de votre WLAN se fait en entrant les paramètres système et les paramètres de communication des postes clients et des différentes bases. Parmi les paramètres système figurent : le nom du WLAN (SSID ou ESS selon le type de réseau sans fil), le mode

1. Wi-Fi est un label délivré par le WECA (*Wireless Ethernet Compatibility Alliance*), un organisme chargé de tester l'interopérabilité des différents équipements.

2. Standard autorisant le *roaming* (déplacement dans des zones couvertes par plusieurs bases) entre des bases provenant de constructeurs différents.

3. Certains équipements proposent une aide pour réaliser ces tests (mode *survey*).

de fonctionnement de l'interface sans fil (en mode constamment actif ou en mode veille pour économiser l'énergie), le type de réseau (réseau à infrastructure). Il faut également choisir les paramètres de communication : le débit (le plus élevé possible ou à spécifier manuellement), les canaux de communication, la taille maximale d'une trame, la puissance d'émission. Les différents champs doivent être remplis en veillant à ce que tous les paramètres soient identiques dans tous les composants du WLAN.

g La sécurité d'un réseau sans fil proposée par les standards 802.11 s'appuie sur : l'identification du WLAN, l'enregistrement des adresses MAC des stations participantes et le chiffrement. Cette sécurité est notoirement insuffisante car elle peut aisément se contourner : l'identifiant est statique et, en outre, il est affiché en clair dans les outils de configuration ; l'adresse MAC peut se changer dans une carte réseau ; quant au chiffrement standard, il utilise une clé WEP, un mécanisme d'authentification très simple qui fait appel à un algorithme de chiffrement facilement cassable… Le standard 802.11i ou encore WPA (*Wi-Fi Protected Access*) offrent une meilleure sécurité car ils s'appuient sur des protocoles d'authentification plus évolués.

WPA est un sous-ensemble du standard 802.11i. Il utilise EAP (*Extensible Authentification Protocol*) et TKIP (*Temporal Key Integrity Protocol*). EAP, décrit dans le standard 802.11x, sert à authentifier les équipements du réseau, et TKIP renforce la sécurité du protocole WEP. Par ailleurs, 802.11i permet d'utiliser un algorithme de chiffrement plus robuste que celui utilisé par la clé WEP.

Cas 3 : Interconnexion des différents sites d'une grosse entreprise

Énoncé

Une entreprise largement déployée sur la région parisienne possède environ 250 sites et 12 000 postes de travail identiques, auxquels il faut ajouter 250 serveurs (à raison d'un serveur par site). Les deux sites les plus éloignés du réseau sont distants de 123 km.

a Peut-on envisager d'utiliser un réseau Ethernet global pour cette entreprise ? Pourquoi ?

b Le directeur du système d'information (DSI) décide d'implanter un réseau Ethernet par site. Un réseau fédérateur FDDI[a] interconnecte tous les réseaux Ethernet de l'entreprise (directement ou indirectement…). Quels matériels d'interconnexion sont nécessaires ? Combien ? Proposez une solution d'interconnexion.

c L'administrateur du réseau demande une adresse IP pour son entreprise. Quelle classe lui faut-il ?

d On lui octroie l'adresse réseau `145.87.0.0`. Cela lui convient-il ? Peut-il prévoir un plan d'adressage avec autant de sous-réseaux qu'il y a de réseaux physiques existants ?

e Le DSI voudrait mettre en œuvre un serveur Web, accessible depuis l'extérieur de l'entreprise. Proposez une localisation possible et un modèle de sécurité pour ce serveur.

f Seuls 3 % des utilisateurs sont effectivement autorisés par la direction à sortir du réseau de l'entreprise et à naviguer sur Internet (toutes applications confondues). Le plan d'adressage précédent est-il utile ? Proposez une solution.

a. FDDI (*Fiber Distributed Data Interface*) est un réseau local utilisant des fibres optiques, qui permet de relier des stations réparties sur plusieurs dizaines de kilomètres à 100 Mbit/s. Il constitue un moyen commode de fédérer les sous-réseaux d'une entreprise.

Solution

a D'une part, la distance entre les sites est trop importante pour constituer un seul réseau Ethernet global. D'autre part, le nombre de stations à connecter dépasse ce qui est prévu dans le standard. Le plus simple est de mettre en place autant de réseaux Ethernet que de

sites, de façon à permettre à chacun d'évoluer en fonction des besoins de ses utilisateurs et du développement de la société. Il vaut donc mieux installer 250 réseaux Ethernet.

b Il faudrait 250 routeurs, un pour chaque réseau, mais cela peut coûter vraiment très cher à l'entreprise ! Pour diminuer le coût de l'installation, on va regrouper les sites 10 par 10. Les regroupements de sites sont reliés au réseau FDDI par de gros routeurs fédérateurs de sites, ce qui limite leur nombre à 25.

c Il lui faut une adresse de classe *B* car il y a 12 000 postes, une adresse de classe *C* étant insuffisante pour couvrir tous les postes (254 postes seulement).

d L'adresse `145.87.0.0` est une adresse de classe *B*, qui permet de connecter au maximum 65 534 postes et routeurs, ce qui est largement suffisant pour la société.

Un plan d'adressage possible serait d'utiliser 251 sous-réseaux (un sous-réseau par site plus un sous-réseau pour le réseau FDDI), numérotés de 1 à 251 : par exemple des adresses réseau allant de `145.87.1.0` à `145.87.251.0`[4].

e Le serveur Web serait idéalement placé à mi-chemin entre les deux sites les plus éloignés. En effet, aucun ne sera désavantagé par rapport à l'autre pour accéder aux pages Web. Le modèle de sécurité à envisager pour permettre les accès extérieurs est le modèle « zone sas » ou « zone démilitarisée » couplé à un pare-feu. Cela permet une protection du réseau interne vis-à-vis de l'extérieur, tout en autorisant des serveurs ou des applications à se connecter à l'extérieur (après configuration).

f Si les 3 % d'utilisateurs autorisés à naviguer sur Internet sont répartis uniformément sur tous les sites et qu'ils possèdent une adresse IP fixe, l'administrateur devra décider, *pour chacun des utilisateurs*, s'il a ou non le droit de sortir du réseau de l'entreprise, ce qui représente un travail long et fastidieux, qu'il faut recommencer dès que le droit de l'utilisateur évolue ! Le plus simple serait de regrouper les utilisateurs habilités à naviguer sur Internet dans certains sous-réseaux et de filtrer l'accès à Internet en fonction des sous-réseaux. Dans ce cas, le plan d'adressage précédent serait sans utilité. Le serveur Web devrait se placer sur le site qui a le plus d'accès externes vers Internet (le site qui possède le plus d'utilisateurs autorisés). Un routeur et un pare-feu bien configurés suffisent à protéger le réseau interne.

Cas 4 : Utilisation de CIDR et du NAT dans l'entreprise

Énoncé

Le responsable du réseau de l'entreprise précédente vous demande de configurer les routeurs, conformément à la solution adoptée.

a Sachant qu'une adresse de classe *B* avait été octroyée à l'entreprise, proposez les masques de sous-réseau utilisables sur les différents routeurs de site.

b Combien peut-on installer de machines par sous-réseau, sachant que dans chaque sous-réseau se trouvent 3 routeurs vers d'autres sites ?

c Plutôt que de vous appuyer sur l'adresse de classe *B*, vous décidez d'utiliser une adresse privée de classe *A* pour identifier machines et routeurs et d'utiliser le NAT pour convertir les adresses privées en adresses routables. Comment justifiez-vous votre choix auprès du responsable ?

d Proposez les masques de sous-réseau dans les différents routeurs (routeurs fédérateurs et routeurs de site) pour les adresses privées.

e Combien de machines peut-on identifier dans chaque sous-réseau avec cette nouvelle solution ?

4. En fait, on utilise beaucoup plus d'adresses réseau si les équipements d'interconnexion sont des routeurs : en effet, ceux-ci possèdent autant d'adresses IP que d'accès aux réseaux qu'ils relient (les routeurs n'assurent le routage qu'entre des réseaux d'adresses différentes). On préfère dans ce cas employer des commutateuurs-routeurs, ce qui simplifie le travail d'administration et économise des adresses réseau.

Solution

a Pour identifier les 251 sous-réseaux, il faut 8 bits. Le masque de sous-réseau est donc : `255.255.255.0`, c'est-à-dire `/24`.

b Il reste un octet pour identifier les machines, chaque sous-réseau compte 254 identifiants à affecter aux machines, moins les 3 adresses IP consommées par les routeurs. On peut donc raccorder 251 machines par sous-réseau.

c D'une part, vous pouvez augmenter considérablement le nombre de machines et d'équipements dans chaque sous-réseau de votre entreprise. D'autre part, vous renforcez la sécurité de votre réseau puisque les machines ne peuvent plus accéder directement à Internet (ni être atteintes). Enfin, l'adressage privé et le NAT vous permettent d'attribuer des adresses aux machines en vous affranchissant des contraintes de routage imposées par les communications avec l'extérieur n'utilisant que des adresses IP routables.

d Il faut 5 bits pour identifier les 25 routeurs fédérateurs. Le masque dans ces routeurs sera : `/13`. Pour identifier les 10 subdivisions de chaque gros routeur, il faut 4 bits supplémentaires. Le masque dans les routeurs de site sera `/17`.

e Puisqu'il reste 15 bits pour identifier machines et équipements dans chaque sous-réseau, on pourra disposer de $2^{15}-2$ adresses IP privées. Avec cette solution, on peut identifier 32 766 machines ou routeurs dans chaque sous-réseau.

Cas 5 : Évolution de l'architecture réseau d'une entreprise

Énoncé

Une petite start-up démarre son activité. Elle commence avec 5 stations de travail multimédia, une station de travail bureautique et un serveur.

a Elle souhaite trouver les solutions les moins onéreuses pour ne pas compromettre sa situation financière, tout en permettant une évolution ultérieure. Quelle architecture de réseau proposez-vous ?

b La société grossit : elle acquiert 10 stations de travail multimédia et 2 stations de travail pour la bureautique. Quelles sont les répercussions de cette extension sur l'architecture du réseau ?

c La société se développe de plus en plus. Elle a acquis, quelques étages plus haut, d'autres locaux situés au même étage. Elle y installe une cinquantaine de postes de travail et 4 serveurs supplémentaires. Indiquez les nouvelles modifications induites par cette évolution.

d La société s'étend très rapidement et occupe désormais les six étages de l'immeuble. On vous nomme responsable du réseau de la nouvelle entreprise. Décrivez votre démarche pour tenir compte des nouveaux besoins du réseau.

e L'extension de la société s'est poursuivie à un rythme accéléré. Il y a désormais des bureaux dans d'autres immeubles voisins. Le nombre de machines croît brusquement et passe à 500. Quelles sont les évolutions à envisager ?

f Dans cette nouvelle situation, des plaintes émanent d'usagers mécontents : les utilisateurs de bases de données client-serveur se plaignent d'une augmentation insupportable du temps de réponse, pendant que les utilisateurs de stations de travail multimédia fonctionnant sous Unix constatent un ralentissement très désagréable du déplacement du curseur sur leurs écrans. Comment a-t-on abouti à cette situation ?

g Votre société continue à prospérer. Fort de votre expérience, vous décidez de ne pas attendre que surgissent de nouveaux problèmes pour faire évoluer votre réseau. Proposez une évolution qui garantisse la continuité du service, même en cas de panne de certains équipements. ☞

Énoncé *(suite)*

h Parallèlement aux problèmes d'architecture du réseau, vous avez élaboré un plan d'adressage pour identifier machines et sous-réseaux de l'entreprise. Indiquez les principes qui vous ont guidé dans vos choix.

i La société a ouvert des bureaux à Lille, Lyon, Marseille et Toulouse. Indiquez les conséquences de cette extension sur le plan d'adressage que vous avez élaboré précédemment.

j Dans votre plan d'adressage, Marseille utilise les adresses `10.20.0.0` à `10.23.0.0`. Sur ce site, on vous demande de créer des réseaux de différentes tailles : un réseau principal ayant au moins 1 000 adresses, un sous-réseau pour regrouper les 20 serveurs du site, 240 petits sous-réseaux dédiés connectés au même pare-feu, la possibilité d'identifier 60 accès distants et 10 accès externes, un sous-réseau pour l'autocommutateur (PABX) de l'entreprise comptant 30 adresses. Proposez une affectation des différentes adresses de sous-réseau et indiquez les masques correspondants.

Solution

a La petite société choisit une solution Ethernet avec des accès à 10 Mbit/s pour les stations de travail bureautique et à 100 Mbit/s pour les stations de travail multimédia et le serveur. Toutes les machines sont équipées de cartes 10/100 Mbit/s. Elles sont connectées par des paires torsadées à un commutateur empilable (*stackable*), doté de 16 ports[5] à détection automatique de vitesse (ports *autosense*[6]). Le commutateur est placé dans un local technique d'étage (LTE).

b Pour accroître son parc de machines, la société acquiert un autre commutateur de même type et de même marque. Dans le LTE, on a placé les deux commutateurs, reliés par un câble externe.

Remarque

Lorsque plusieurs commutateurs sont chaînés entre eux afin d'augmenter le nombre de stations connectées, ils se servent d'un bus dédié qui utilise le plus souvent un protocole propriétaire : il est donc prudent d'acheter ces équipements chez le même constructeur. La plupart du temps, on peut relier jusqu'à 8 commutateurs avec cette technique.

c Pour connecter tous les postes du nouvel étage, on utilise deux commutateurs à 32 ports de même marque que les précédents, qu'on place dans un LTE, contenant également tous les serveurs de l'étage. Chaque serveur est directement raccordé à un port d'un commutateur. Il faut ensuite raccorder les deux étages entre eux. Pour cela, on relie les deux LTE par un *câble de rocade*.

d Dans un premier temps, on peut envisager d'installer un réseau local par étage. Cette politique est à très courte vue, pour plusieurs raisons : on atteint vite les possibilités de mise en cascade des différents commutateurs, les performances du réseau Ethernet vont s'effondrer à cause d'un nombre inacceptable de collisions (cette éventualité surgit à partir d'une centaine de stations connectées), entraînant des temps de réponse trop grands. Il faut donc installer un *réseau fédérateur* (*backbone*).

Une première solution pourrait être le déploiement d'un réseau FDDI, comme celui de l'exercice 3. Vous ne retenez pas cette solution, car vous considérez que cette solution vous cantonnerait à un débit de 100 Mbit/s dans le réseau fédérateur. Or, vous supposez que la forte croissance de la société va se poursuivre et que vous devrez assez vite envisager des solutions à 1 Gbit/s. Vous choisissez donc une architecture de type *collapse backbone* : un

5. Les concentrateurs ou les commutateurs ont le plus souvent 8, 16, 24 ou 32 ports.

6. Les cartes réseau 10/100 des machines peuvent poser des problèmes aux commutateurs dotés de ports *autosense* : il vaut mieux désactiver la fonction *autosense* de la carte réseau et choisir manuellement la vitesse.

unique et puissant commutateur sert à connecter tous les étages. Pour cela, vous concevez une architecture en étoile à deux niveaux : le premier niveau regroupe toutes les machines d'un étage ; le second niveau regroupe dans une même salle, la salle informatique (SI), tous les équipements réseau et les serveurs. Cette solution restera valable pour connecter jusqu'à quelques centaines d'utilisateurs.

e Il faut maintenant améliorer la sécurité de fonctionnement du réseau car ce dernier constitue désormais une ressource vitale pour l'entreprise. Pour augmenter la fiabilité du réseau fédérateur, on va faire l'acquisition d'un autre commutateur, identique au précédent et susceptible de prendre la relève en cas de défaillance. Les deux commutateurs seront reliés par un *trunk* à très haut débit, par agrégation de plusieurs ports Gigabit (*port trunking*).

D'autres facteurs doivent être pris en compte : le réseau doit continuer à fonctionner, même en cas d'incidents comme des pannes d'alimentation, des coupures de câbles entre commutateurs, un débranchement intempestif de *transceivers* (équipements assurant l'émission/réception dans un réseau Ethernet)… Il faut donc mettre en place des solutions réseau redondantes, selon le degré de sécurité souhaité : tout d'abord un système de câblage qui offre plusieurs chemins possibles, la disposition d'équipements de secours qui prennent la relève automatiquement (en utilisant le protocole VRRP par exemple), la redondance des serveurs, voire le doublement des cartes réseau dans les stations de travail les plus critiques. Dans ce dernier cas, la station est dotée de cartes deux ports : dès que le premier port perd le contact avec le commutateur habituel, il bascule sur le second port, relié à un autre commutateur. Pour les serveurs, l'utilisation de ce type de carte permet par exemple un partage de charge en fonctionnement normal (voir chapitre 5, exercice 20).

f Cette situation se produit lorsque la brusque montée en charge du réseau a été sous-estimée. En effet, les utilisateurs d'applications grandes consommatrices de bande passante (par exemple celles qui utilisent de grosses bases de données) perturbent les autres trafics. L'utilisation systématique des commutateurs depuis le début a permis de segmenter le réseau mais l'isolement des différents trafics a été mal fait.

g Dans un premier temps, il faut mieux répartir les flux entre les différents VLAN, en tenant compte des trafics réellement engendrés par les différents utilisateurs ou groupes d'utilisateurs. Éventuellement, il faut revoir la capacité ou la redondance du réseau fédérateur, sans attendre l'engorgement d'une partie du réseau.

Pour cela, l'architecte doit surveiller de près l'évolution des trafics et anticiper les problèmes, en conciliant deux objectifs contradictoires : offrir un service réseau satisfaisant pour tous les utilisateurs, du plus gourmand au plus modeste, tout en ne grevant pas de manière insupportable le budget de fonctionnement de l'entreprise. Il doit au besoin prévoir une politique d'acquisition d'équipements qui s'étale sur plusieurs années. Il est donc très important de bien choisir les technologies, car toute erreur paralyserait l'évolution du réseau et le rendrait obsolète à moyen terme. En outre, il faut choisir avec soin ses fournisseurs, d'une part pour ne pas dépendre d'un seul équipementier pour les équipements stratégiques du réseau et, d'autre part, pour garantir la compatibilité de fonctionnement des matériels qui communiquent.

h Pour élaborer un plan d'adressage qui ne sera pas remis en cause chaque fois que le réseau évolue, il vaut mieux utiliser un adressage privé défini par la RFC 1918. Vu le rythme de croissance très rapide de la société, vous décidez d'utiliser une adresse privée de classe *A* pour vous laisser une marge de progression importante dans l'évolution du réseau. Vous utilisez donc l'adresse réseau : `10.0.0.0 /16`, permettant d'affecter 8 bits pour identifier les sous-réseaux, ce qui revient à utiliser un adressage de classe *B*.

Pour simplifier votre plan d'adressage, vous décidez de choisir au moins une adresse de sous-réseau par site, les sites les plus importants comprenant éventuellement plusieurs adresses de sous-réseau. Dès le départ, vous utilisez 8 adresses de sous-réseau pour le

siège, les adresses allant de `10.0.0.0` à `10.7.0.0`. Au sein de chaque sous-réseau, vous avez la possibilité de créer des subdivisions pour adresser de petits sous-réseaux dédiés (correspondant par exemple à des réseaux de classe *C*). Ces petits sous-réseaux pourront eux-mêmes être découpés en tout petits réseaux, si on veut connecter un seul routeur et quelques machines entre eux.

i Le fait d'installer des réseaux dans d'autres villes ne remet pas en cause votre plan d'adressage précédent. Si vous prenez par exemple 4 adresses de sous-réseaux par nouveau site, vous utiliserez les adresses allant de `10.8.0.0` à `10.23.0.0` pour vos différents sites.

j Tout d'abord, vous décidez de conserver les adresses `10.21.0.0` à `10.23.0.0` pour un déploiement futur, de façon à ne pas être pris au dépourvu pour avoir sous-dimensionné votre plan d'adressage. Vous découpez l'adresse `10.20.0.0 /16` de la façon indiquée au tableau 11.4. Remarquons au préalable que l'identification des différents sous-réseaux de l'entreprise contient 6 bits communs dans le deuxième octet. On utilise donc pour le site de Marseille l'adresse : `10.20.0.0 /14`. Les subdivisions suivantes tiennent compte des hypothèses de travail formulées. Par prudence, vous réservez, au sein de l'adresse choisie (`10.20.0.0 /14`), des plages d'adresses disponibles pour un agrandissement ultérieur avant d'employer les autres adresses du site.

Tableau 11.4 ***Affectation des différentes adresses de sous-réseau en fonction des sites***

Affectation d'adresses	Adresse et masque	Possibilités	Commentaires
Réseau principal	10.20.0.0 /22	1 024 adresses IP[a]	Adresses disponibles dans le réseau
Extension du réseau	10.20.4.0 /22	1 022 adresses IP	Réservé pour une évolution future
Petits réseaux dédiés[b]	10.20.8.0 /24	254 adresses IP	Derrière le même pare-feu
Serveurs du site	10.20.8.0 /27	30 adresses IP	Subdivision du réseau `10.20.8.0 /24`
	10.20.8.32 /27	30 adresses IP	Réservé pour une évolution future
Accès distants	10.20.8.64 /26	62 adresses IP	Identification des accès distants
Accès externes	10.20.8.128 /28	14 adresses IP	Identification des accès externes
	10.20.8.144 /26	14 adresses IP	Réservé pour une évolution future
PABX	10.20.8.160 /26	30 adresses IP	
	10.20.8.192 /26	62 adresses IP	Réservé pour une évolution future

a. En utilisant le masque `/22`, nous indiquons implicitement que les adresses de sous-réseau vont de `10.20.0.0` à `10.20.3.0` pour identifier les 1 024 machines ou routeurs du réseau principal.

b. Le réseau `10.20.10.0 /23` peut lui-même se subdiviser en deux sous-réseaux de classe *C*, par exemple `10.20.10.0 /24` et `10.20.11.0 /24`, pouvant se subdiviser eux-mêmes en tout petits réseaux.

Résumé

Ce chapitre se veut une synthèse des notions développées dans les chapitres précédents. Il explique, sous un angle plus pratique, une approche des problèmes d'administration et de conception d'un réseau. Les études de cas abordent divers aspects, d'une manière plus concrète que lors des chapitres précédents. Il décrit la démarche qui permet de prendre les décisions nécessaires à la construction et à l'évolution d'un réseau, quelle que soit sa taille.