

13. Exercice: architecture d'un réseau d'entreprise



13.1. L'exercice - 13.2. [Architecture globale du réseau](#) - 13.3. [Connexions du réseau administration - commercial](#) - 13.4. [Connexions bâtiment fabrication - commande](#) - 13.5. [Connexion globale de réseau](#) - 13.6. [Un autre point de vue: mélange de protocoles sur le réseau](#)

<p>YBET déménagement Rue Albert 1er, 7 6810 Pin - Chiny Route Arlon - Florenville (/fax: 061/32.00.15</p>		<p><u>Stockage, manutention, sécurité</u> l'indispensable pour votre entreprise</p>
<p>Le <u>cours HARDWARE 2</u> d'YBET Informatique: Serveurs, réseaux et communication</p>		
FORMATIONS	Le MAGASIN YBET	PRODUITS et SERVICES
COURS HARDWARE	Activités et présentation	Caisses enregistreuses et balances TEC
Dictionnaire technique réseaux et communications	Rayon d'action	MATERIEL INFORMATIQUE
Formation INTERNET		Logiciel de gestion CIEL et SAGE
ACCUEIL	Forum informatique technique	Achat en ligne?

13.1. L'exercice

Ceci est l'examen de l'année 2002-2003 du cours hardware de deuxième année. Comme la théorie sans la pratique ne sert pas à grand chose, voyons un cas concret de l'architecture d'une installation réseau (appareils à mettre en oeuvre) dans une entreprise. L'examen se fait avec l'accès au cours. Nous utiliserons les chapitres suivants.

[Les concentrateurs Ethernet](#): Hardware 2 chapitre 5

[Les spécificités serveurs](#): Hardware 2 chapitre 7

[Stockage et sauvegarde en réseau](#): Hardware 2 chapitre 9

[Connexion à distance, sécurité et partage](#): Hardware 2 chapitre 10

[Les communications sans fils](#): Hardware 2 chapitre 11

[Les protections électriques](#): Hardware 2 chapitre 12

Ceci rassemble pratiquement l'ensemble du cours hardware 2, sauf le paramétrage des appareils. Le chapitre 17 avait servi d'examen pour l'année 2001-2002.

La Question de l'exercice

2 bâtiments à connecter distants de 80 mètres (pas de chance, une route au milieu). Chaque bâtiment dispose de deux étages avec 2 départements différents (soit 4 départements). Je veux absolument des niveaux de sécurité (hardware) pour que chaque PC d'un département ne puissent (sauf autorisation par station de travail) se connecter sur un autre département. Cette solution de protection sera en pratique couplée avec des protections logicielles qui sont repris dans les autres cours "Technicien PC / Réseau".

Les départements sont

1. **Bâtiment 1**: 80 PC de fabrication (pas d'accès INTERNET) et 1 serveur avec un logiciel dédié. Distance maximum avec le serveur 100 mètres que nous appellerons **Fabrication**. Ce département rassemble la fabrication, les stocks, gestion des transports, ... C'est le département à protéger. Un arrêt d'usine de 1 heure coûte nettement plus chère à l'entreprise qu'un arrêt de 2 jours de la comptabilité.
2. **Bâtiment 1**: 10 PC de gestion de commandes et 1 serveur dédié. Certains d'entre eux peuvent avoir accès au service du serveur de la fabrication sur un rayon de 30 mètres. Pas d'accès INTERNET, ni vers le bâtiment 2. Nous appellerons ce département **commande**
3. **Bâtiment 2**: 10 PC administratifs: direction, comptabilité, ... sur un rayon de 30 mètres. Nous appellerons ce département **Administration**
4. **Bâtiment 2**: 10 commerciaux. et services divers sur un rayon de 30 mètres. Nous appellerons ce département **commercial**.

Le bâtiment 2 abrite un petit serveur de fichier (documents Word, Excell, ...) et un serveur d'application (comptabilité), appelé **serveur administratif**. Certains PC peuvent avoir accès au serveur "gestion de commande". Le bâtiment 2 (administration et commercial) doit avoir un accès sécurisé sur INTERNET via une ligne ADSL. Il doit être possible pour les commerciaux de se connecter au serveur de l'entreprise à distance via INTERNET.

Je ne parle pas de sécurité via mots de passe, mais bien par des paramétrages TCP/IP ou des matériels informatiques. C'est nettement plus sûr, même si les mots de passe utilisateurs sont loin d'être facultatifs.

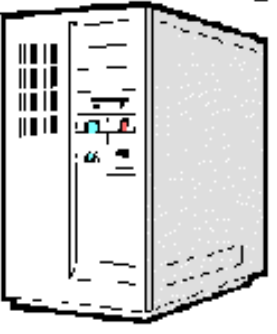


Donnez le schéma de l'installation reprenant les serveurs, concentrateurs utilisés (hub, switch, routeur, nombre de ports), types de liaisons, câbles droits ou croisés, ... Dans le cas où vous utilisez un HUB ou un switch, expliquez. Je ne demande pas explicitement la marque et l'appareil de chaque concentrateur. Attention qu'un switch de 80 ports, ce n'est pas courant, manageable?


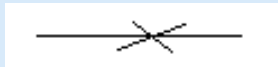


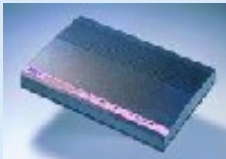





L'installation du réseau doit être complète, pensez aux sécurités à installer (protections électriques, sauvegarde) et aux types de serveurs utilisés. Comme le matériel informatique réseau peut tomber en panne, le matériel doit être standardisé (par exemple les switch) pour que l'on puisse utiliser un minimum de matériel de réserve: maximum de concentrateurs de même type et capacité pour l'ensemble du réseau pour n'utiliser qu'un appareil de remplacement pour toute l'entreprise. Je ne demande pas les paramétrages des appareils, juste la structure du réseau ethernet.

Ne vous occupez pas trop du budget, mais choisissez les caractéristiques en gestionnaire informatique responsable (pas la peine d'utiliser de l'Ethernet Gigabit sur fibre optique pour connecter les stations).

2. L'architecture globale.

Pour faciliter la mise en place de l'architecture de notre réseau, examinons les appareils à mettre en oeuvre. Nous utiliserons les dessins suivants pour faciliter l'analyse du schéma global du réseau.

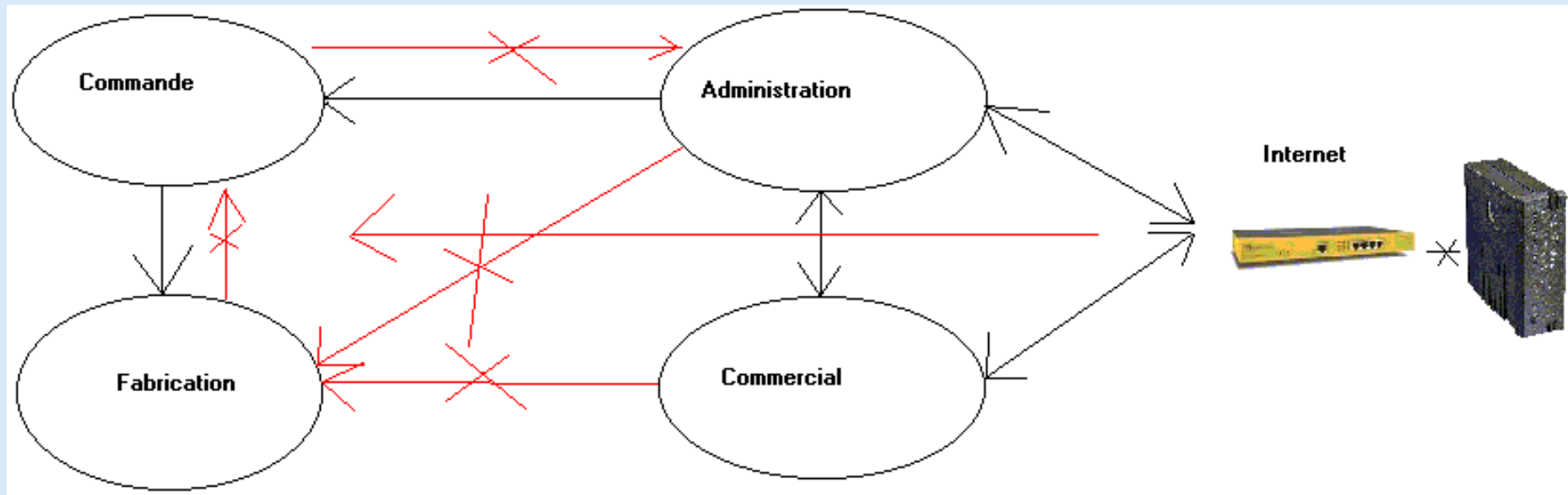
		
<p>Serveur</p>	<p>Switch ou Hub Ethernet (ici un des 1024d de Dlink 24 ports 10/100)</p>	<p>Switch manageable: autoriser (ou bloquer) certaines connexion de PC vers PC (ou plutôt de groupes de PC), en plus des mots de passe sessions utilisateurs gérés par le système d'exploitation</p> <p>Ici un DGS 3224, 20 ports 10/100 et 2 ports Gigabits en base T (cuivre) de Dlink</p>

			
<p>Routeur sans fils Wifi, utilisable comme routeur et comme pont. Nous pourrions utiliser un simple switch sans fils dans notre cas.</p>	<p>Un câble RJ 45 croisé</p>	<p>modem routeur ADSL, ici un tornado Copperjet 812. Il peut être utilisé comme simple modem en mode pont</p>	<p>Un firewall - VPN (ici une série 100 de symantec) permet le partage de la connexion Internet et l'accès de l'extérieur au réseau de l'entreprise</p>
			
<p>Routeur firewall intégré permet de sécurisé les connexions en bloquant certains ports et / ou certaines pages d'adresses.</p>	<p>un simple routeur</p>	<p>NAS (ici un série 300 low cost de IOMEGA)</p>	<p>Un département avec les PC associés</p>
			
<p>UPS (ici APC 420W, un peu faible pour un serveur): protection électrique</p>	<p>Sauvegarde sur bande SDLT (ici modèle Quantum)</p>		

Analysons le problème en fonction des différentes parties et des sens de communication autorisés. Ceci va scinder le problème et envisager en gros les appareils à utiliser au niveau connexion, routage et sécurité.

Les départements administration et commerciaux ne sont pas très différents. Ils utilisent tous deux: INTERNET (ce sont les seuls), les mêmes serveurs (un serveur de fichier et un petit serveur d'application). Par contre l'administration doit pouvoir se connecter sur le département commande (mais pas sur le département fabrication), le département commercial ne peut en aucun cas se connecter sur les départements commande et fabrication. L'accès d'INTERNET vers les serveurs du bâtiment 2 (administration et commercial) nous oblige à utiliser un firewall VPN pour la connexion INTERNET (ici un série 100 de symantec) et un modem ADSL (ici un tornado

812 utilisé en pont ([voir chapitre 17](#)). Avec les 20 PC repris dans le bâtiment 2, il n'y a pas besoin d'un appareil très puissant, mais suffisamment sécurisé. Comme l'accès de l'extérieur est possible, la connexion doit être de type IP fixe. Ceci nous donne une bonne marche de manoeuvre pour les connexions.



En noir les communications autorisées (même avec des blocages), en rouge celles qu'il faut bloquer. On a déjà une bonne idée de la structure globale de l'installation. La route entre les deux bâtiments va nous bloquer avec une liaison sur cuivre ou fibre optique. Nous devons déjà utiliser une liaison sans fils, de type WIFI 802.11B à 11 Mb/s (éventuellement 802.11B+ à 22 Mb/s). Comme les vitesses de communications ne sont pas trop importantes, l'utilisation de 100 base T (éventuellement 1000 Base T pour les serveurs) est suffisante pour l'ensemble du réseau.

13.3. Connexions département administratif et commercial

La connexion entre administration et commercial doit laisser passer certaines communications (mais pas toutes). En plus, ils utilisent les mêmes serveurs. Nous pouvons utiliser soit deux classes d'adresses différentes (d'où l'emploi de routeurs pour relier les 2 départements), soit un switch manageable (et donc bloquer ou autoriser certaines connexions) en utilisant la même classe d'adresses IP. Utiliser 2 routeur pour les communication alourdi directement le paramétrage. Choisissons la solution même classe d'adresse (par exemple 192.168.10.X) pour l'ensemble des deux départements et bloquons les accès au niveau d'un switch manageable.

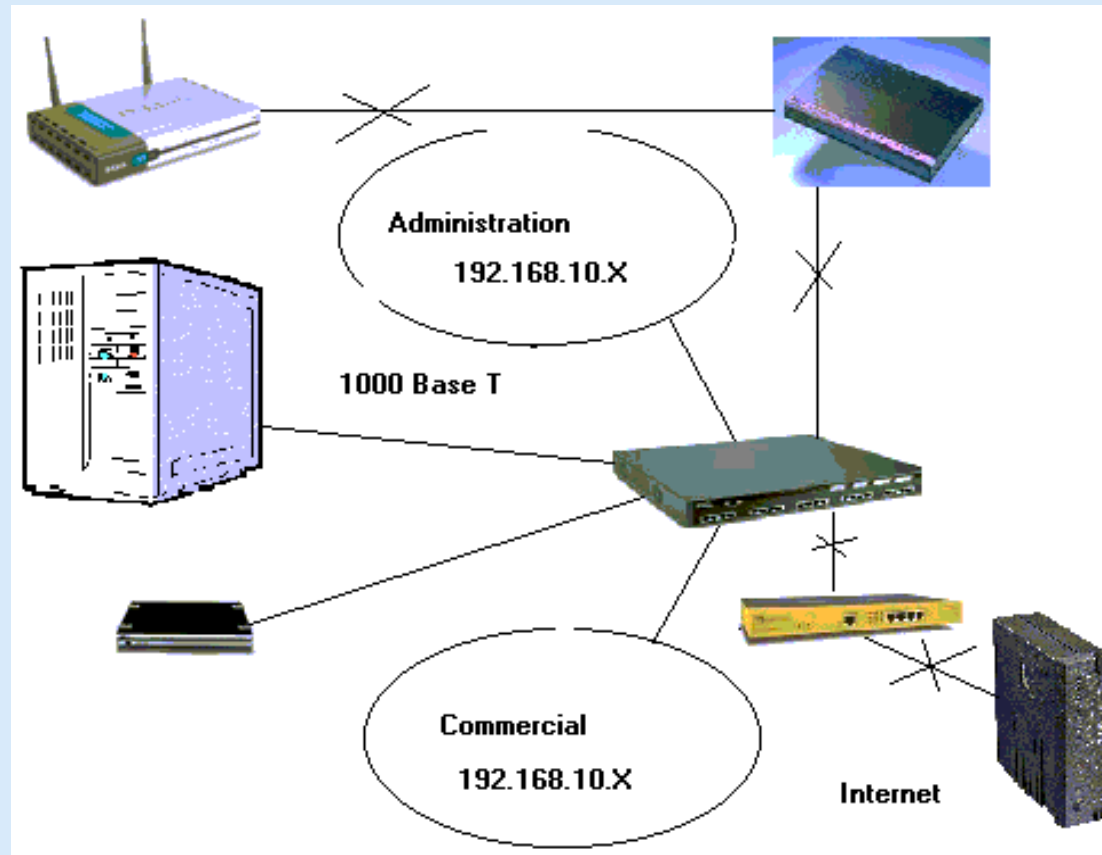
Les départements utilisent un serveur d'application et un petit serveur de fichier. Comme serveur de fichier, pour réduire les coûts, utilisons un NAS. Comme nous devons connecter 20 PC + 1 serveur + 1 NAS + 1 connexion bâtiment 1, l'appareil représenter (20 ports + 2 Giga) serait insuffisant mais nous pourrions utiliser un switch 8 ports additionnels. Les NAS sont rarement en 1000 Base T.

Voyons maintenant la connexion vers le deuxième bâtiment. Nous devons utiliser une connexion sans fils. Comme le bâtiment 2 peut avoir la connexion vers le département commande (pas fabrication, mais pas l'inverse, nous allons utiliser des classes d'adresses différentes pour le bâtiment 1. Ceci nécessite l'emploi d'un routeur. Comme la connexion doit être sécurisé (bloquée à partir du bâtiment 1 vers 2) plus l'interdiction de connexion INTERNET vers le bâtiment 2, utilisons un

routeur firewall et un routeur 802.11B en pont. Dans ce cas, le firewall ne va pas être utilisé pour bloquer des ports: dans un réseau interne, les ports dynamiques (1024 - 65535) sont utilisés de manière aléatoire pour les communications réseaux internes, nous ne pouvons pas les bloquer. Nous allons uniquement bloquer les communications sur les plages d'adresses. Par exemple bloquer les communications de l'adresse IP du VPN vers le bâtiment 2.

Une autre solution pour bloquer l'accès "Fabrication" - "administratif" serait de sécuriser le réseau sans fils en fonction des adresses [mac](#) des PC du département administration, voire [sécurité des réseaux sans fils](#) dans la rubrique [How to?](#)

Voici notre schémas matériel réseau pour le bâtiment 2.

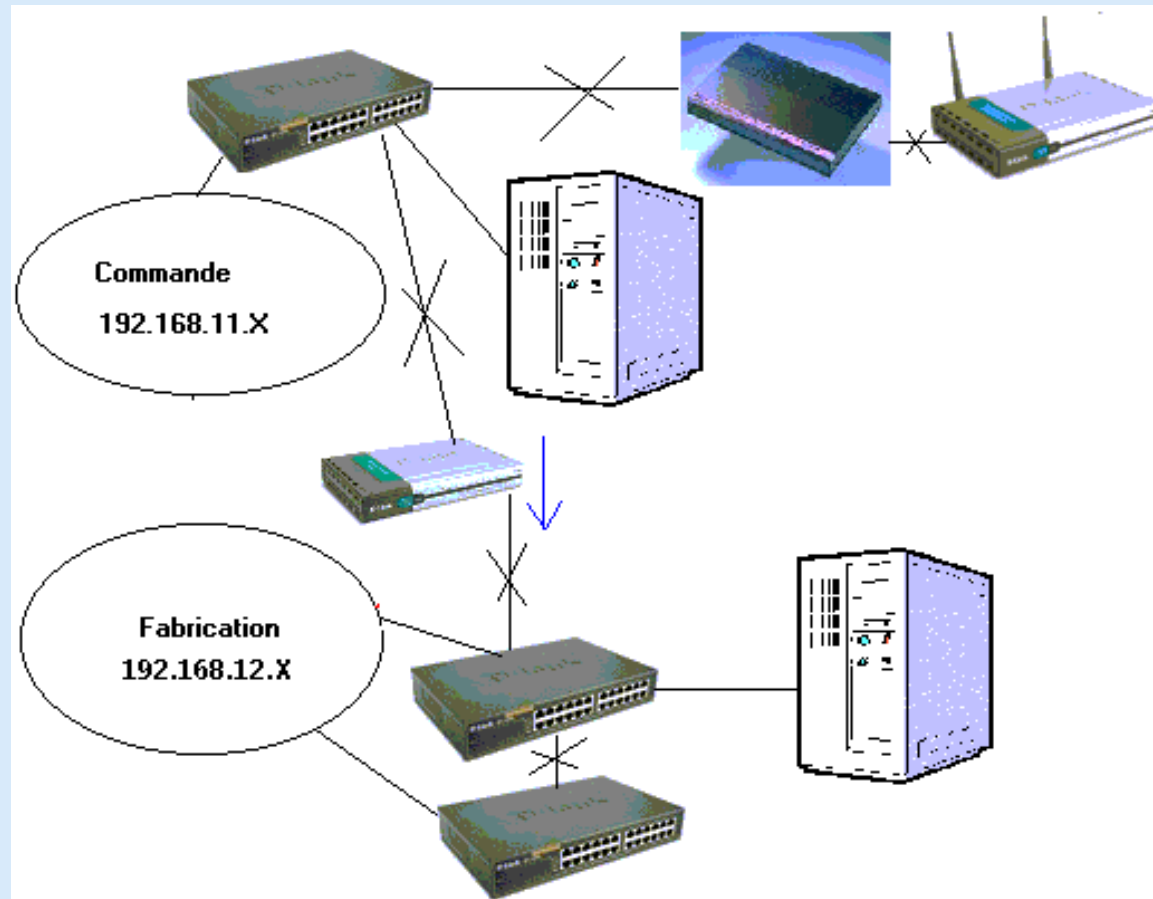


13.4. Connexion Bâtiment fabrication - commande

Les communications usine vers commande sont interdites. Seules les communications commandes vers usines sont autorisées (sous certaines réserves). Nous avons de nouveau deux possibilités d'utilisation des classes d'adresses IP. Soit deux classes différentes avec l'emploi de routeur, soit la même classe d'adresse avec un switch manageable (au choix).

Cas 1: utilisation de 2 classes d'adresses différentes.

L'utilisation d'un routeur (et donc 2 classes d'adresses) va augmenter la sécurité. L'utilisation d'un routeur avec firewall n'est pas obligatoire puisque la communication bidirectionnelle nécessite deux routeurs alors que nous utilisons la communication uniquement de commande vers fabrication. Ceci empêche déjà l'usine de se connecter vers le département commande. La sécurité à partir d'Internet est déjà assurée pour rappel avec le VPN et le firewall placé à la sortie du bâtiment administratif vers le routeur WIFI. De même, pour les communications du bâtiment 1 vers le bâtiment 2, nous pouvons soit utiliser un routeur WIFI en mode pont et un firewall (cas ci-dessous), soit un routeur WIFI sans firewall. La sécurité est de toute façon assurée par le firewall de l'autre côté de la liaison sans fils.



Le nombre de switch 24 ports pour la partie fabrication a volontairement été réduite pour la clarté du schéma. Il nous en faudrait minimum 4, voire 5 pour avoir des lignes de réserves. L'utilisation d'un seul switch de 96 ports pourrait poser des problèmes de longueur de câbles et en cas de panne de ce seul appareil, toute la fabrication serait bloquée. L'utilisation de multiples switch 24 ports permet d'en avoir 1 de réserve pour l'ensemble du bâtiment.

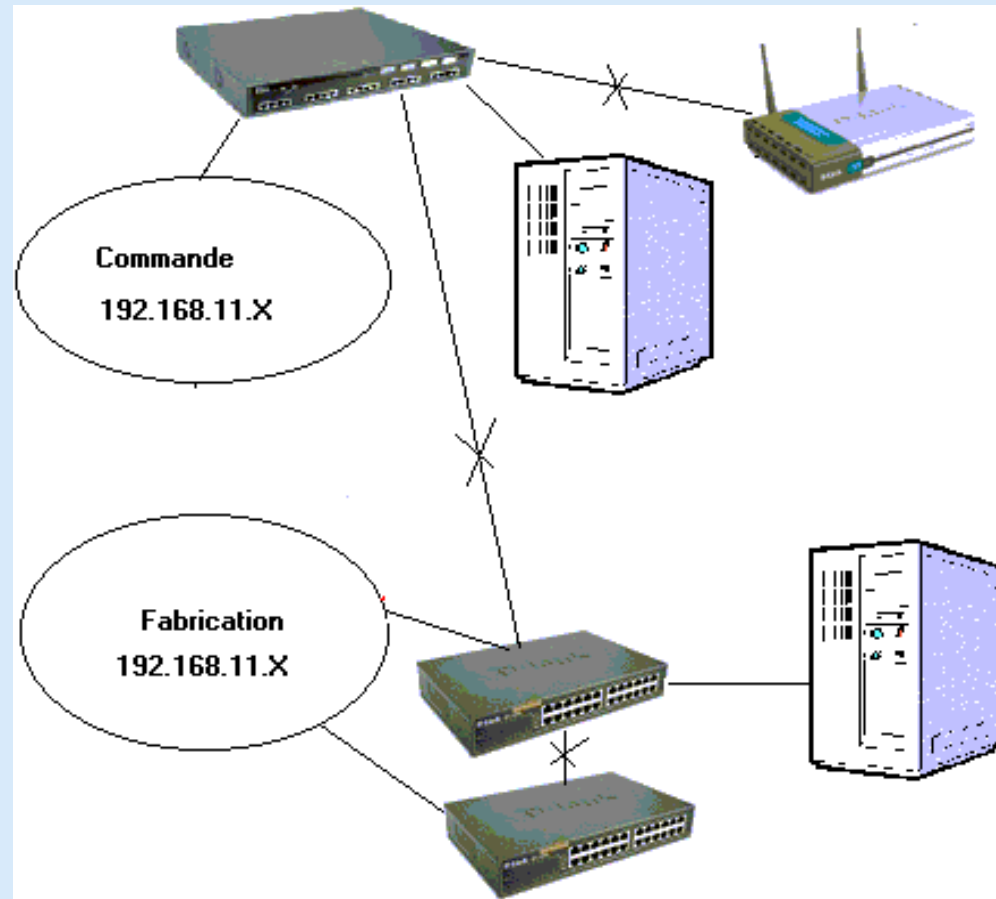
Pour rappel, le nombre de HUBS (moins de contrainte pour les switch) est limité à maximum 2 entre 2 PC en 100 base T (même si plus est souvent utilisé), le serveur

fabrication **doit être raccordé sur le premier switch** de la fabrication

L'utilisation d'un routeur firewall entre le switch et la connexion WIFI 802.11B n'est pas nécessaire si un firewall est installé de l'autre côté. Ils feraient double emploi (ce qui n'est pas trop grave) mais obligerait une configuration plus complexe de l'infrastructure.

Cas 2: utilisation d'une même classe d'adresse avec switch manageable.

Dans ce cas, tous les PC sont dans la même classe d'adresse, l'utilisation d'un routeur (ou routeur - firewall) n'est plus nécessaire entre les deux départements., c'est le switch manageable qui va accepter ou bloquer les communications. Dans ce cas (et contrairement à la solution précédente), on peut bloquer les communications de manière hardware entre les PC des commandes et les PC de fabrication).



Cette solution est nettement plus chère (mais plus sécurisée). Elle permet néanmoins de raccorder les serveurs en 1000 base T sur le switch manageable. Les distances entre chaque PC, serveurs et concentrateurs sont respectées puisque qu'en 100 base T en 1000 base T, la distance maximum est de 100 mètres. Pour rappel, **les switch**

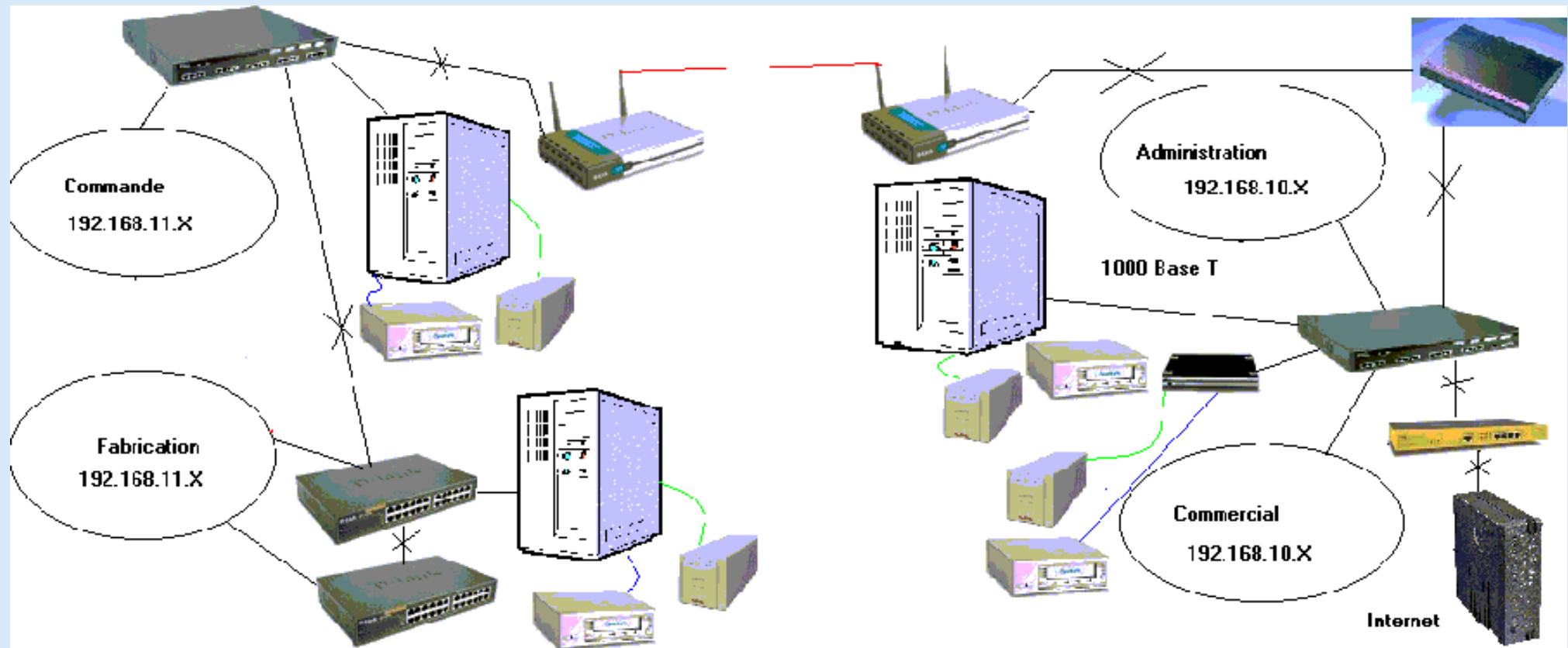
manageables travaillent généralement avec les adresses MAC. En cas de panne d'un PC avec échange standard (ce qui se fait en pratique pour minimiser l'arrêt), on risque de devoir reprogrammer le switch. Ce n'est pas forcément du niveau de tous les techniciens de maintenance d'usine (sans compter les mots de passe administrateurs pour paramétrer le switch). Par contre, certains modèles acceptent le regroupement de station suivant le protocole IGMP.

13.5. Connexions globales du réseau

Il ne reste plus qu'à relier les 2 réseaux de l'entreprise et positionner nos sécurités (UPS et sauvegarde) et choisir les serveurs.

Les serveurs utilisés pour le bâtiment 2 et les commandes sont en fait de petits serveurs. Par contre, le serveur utilisé en fabrication est un serveur d'application musclé (avec logiciel dédié) de type bi-processeur. Pour des raisons de sécurité des données, nous utilisons des serveurs SCSI RAID 1 ou mieux RAID 5. Plus le processeur est gros plus il consomme. L'UPS (de type On-Line de préférence) devra être en rapport. Pour rappel, la puissance de l'UPS = puissance consommée par le serveur X 1,6. Pour un serveur consommant 800 W (écran compris), la puissance de l'UPS est donc de $800 \times 1,6 = 1280$ W.

Pour la sauvegarde des données, nous utiliserons des bandes de type DAT ou Super DLT pour les capacités de ces technologies, mais également au niveau vitesse de sauvegarde.

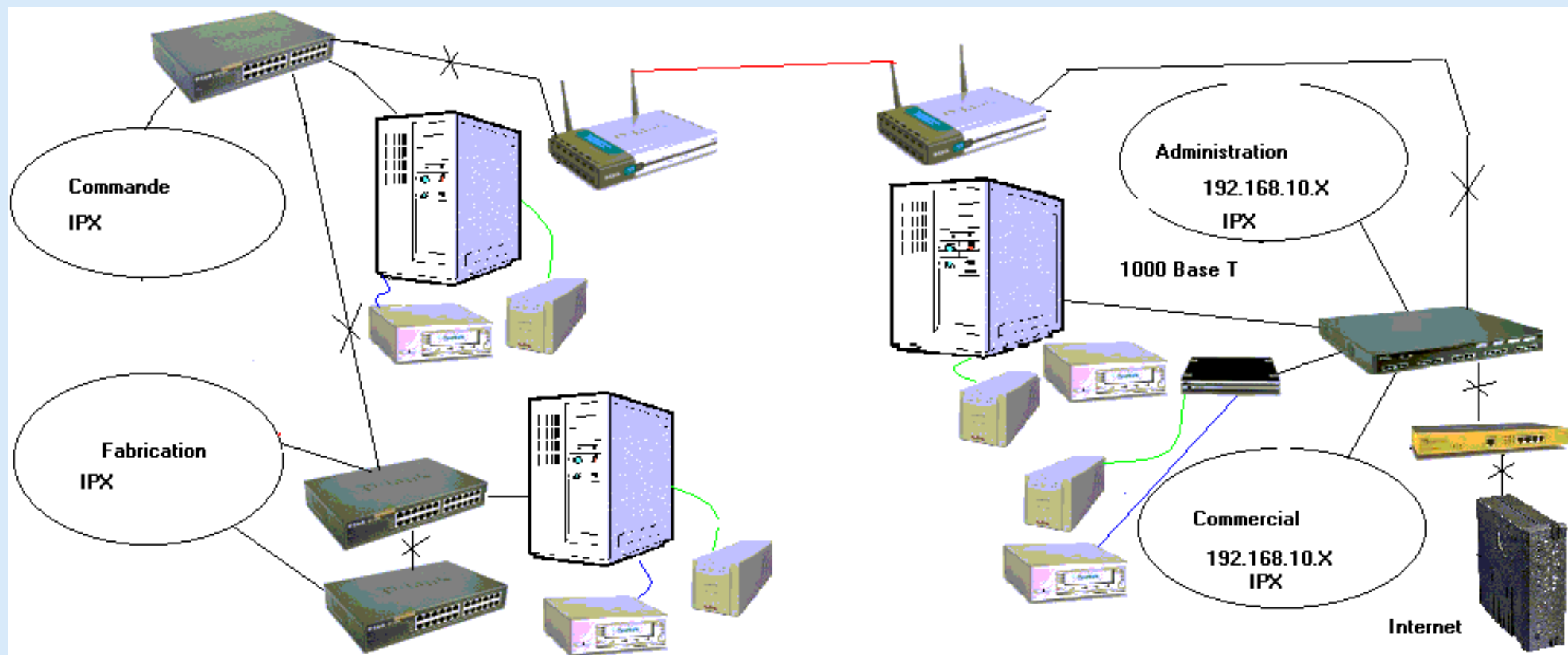


Nous pourrions encore ajouter sur le schémas des petits UPS pour certaines stations ou concentrateurs, selon les desiderata de l'entreprise.

13.6. Un autre point de vue de cette connexion: mélange de protocoles.

Dans les montages ci-dessus, nous avons utilisé exclusivement le protocole TCP/IP. Il en existe 2 autres: l'IPX et le NetBeui. Le NetBeui n'est pas routable, l'IPX (utilisé principalement par les réseaux NOVELL), oui. Le schéma suivant va mélangé des protocoles. Pour accéder à un serveur, le PC doit utiliser le même protocole (mais il peut en utiliser plusieurs en même temps).

Dans le cas du bâtiment 2 administratif, comme on utilise Internet, TCP/IP est obligatoire. Par contre, dans le bâtiment 1 (commande et fabrication), INTERNET est interdit en sortie comme en entrée (intrusion). Nous allons nettement réduire le nombre d'appareils en utilisant dans le bâtiment 1 uniquement IPX et pour le bâtiment 2, les PC qui doivent se connecter sur la partie commande utiliserons IPX et TCP/IP. Cette façon de procéder bloquera toutes les tentatives d'intrusion directes d'Internet vers le bâtiment 1. Par contre, la connexion du département commande vers Fabrication (et vis versa) sera uniquement bloqué par les droits de sessions et les communications pourront également passer du bâtiment 1 vers les PC IPX du bâtiment 2. Il suffit de bloquer les partages dans le bâtiment 2 en IPX.



Dans ce cas, nous remplaçons un switch manageable par un simple switch (avec d'autres du même type utilisés sur l'ensemble du réseau) et plus aucun firewall dans l'ensemble du réseau (à part le VPN pour INTERNET). Cette solution n'est pas à envisager pour une usine de 500 PC, mais bien pour des moyennes structures. Les utilisateurs de réseaux NOVELL privilégieront probablement cette solution.

13.7. Les erreurs et remarques de l'examen

Après correction, je reprend les erreurs de l'architecture du réseau. Sont reprises ici quelques remarques et erreurs de l'examen.

1. Réseau bâtiment 2: 2 classes d'adresses IP différentes pour administratif et commerciaux reliés tous deux sur les ports d'entrée du VPN (connexion INTERNET correcte) mais pas de routeur entre les deux. Dans ce fait, pas d'interconnexion entre les 2 groupes de PC mais plus grave, 1 seul département sur les 2 aura accès au serveur et au NAS. Bref, **l'infrastructure bâtiment 2 ne fonctionne pas**.
2. 2 classes d'adresses différentes pour commande et fabrication. Les PC commandes branchés sur un routeur 16 port (suis pas sûr que cela existe) et branché sur un HUB 8 port qui est relié sur 5 hub 24 ports pour la fabrication. Comme le serveur Fabrication est une application dédiée, on présume que les PC ne se connecteront pas entre eux mais tous vers le serveur à leur tour avec quelques problèmes de collisions (le serveur répondra à chacun à son tour, ce qui peut être correct). Par contre, l'utilisation d'un Hub comme tête de pont entre le routeur commande et les différents HUB fabrication va directement ralentir l'ensemble du réseau.
3. Utilisation de **2 firewall** (1 de chaque côté du pont **WIFI**), configuration de l'architecture du réseau plus complexe.

[Cours: Les concentrateurs Ethernet](#)

Hub, switch, routeurs, ...

[Cours: Spécificités serveurs](#)

Architecture, mémoires, ...

[Cours: Réseaux Ethernet](#)

Normes des réseaux Ethernet

[Cours: communications sans fils](#)

Communications sans fils, normes, vitesses, ...

La suite du cours Hardware 2 > [Chapitre 14: Technologies spécifiques](#)



Pour l'ensemble du [cours hardware](#)

Le [cours "Hardware 1"](#): PC et périphériques, le [cours "Hardware 2"](#): Réseau, serveurs et communication.

Pour l'ensemble du [site YBET informatique à Florenville \(info, se dépanner, ...\)](#)

© YBET informatique 2004

