Réseau local (Corrigé)

6. CORRIGÉS

1. Étude de cas

a. Les outils de bureautique et de gestion utilisés une PME tendent à nous faire opter pour une architecture de la famille Ethernet, la plus répandue dans un tel contexte.
Aucun réseau n'est actuellement installé dans ce service, aucune précision n'est fournie concernant la quantité d'information devant transiter sur ce réseau : il semble alors judicieux de mettre en place une architecture Fast Ethernet, suivant la norme IEEE 802.3u, celle-ci proposant des atouts technologiques intéressants, et une forte capacité d'évolution.

b. Chaque poste de travail doit être muni d'une interface réseau Fast Ethernet. Il en est de même pour le serveur.
Un concentrateur (hub) ou commutateur (switch) permet d'interconnecter tous les ordinateurs. On choisit pour des raisons d'évolutivité un hub ou switch disposant de plus de ports d'entrée/sortie que d'ordinateurs à connecter (16 ports par exemple).
La distance séparant les ordinateurs du hub étant de manière évidente inférieure à 100 mètres, on utilise pour la connexion du câble à paires torsadées de Catégorie 5 à connecteurs RJ45. Les ports d'entrée/sortie du hub doivent donc être aux aussi au format RJ45.

c. Une première solution (*Fig. 7.48. (1)*) simple mais très peu évolutive consiste à ajouter quatre liaisons supplémentaires entre les postes de travail et le hub en place, ce qui conserverait une topologie parfaitement homogène. La distance de 120 mètres ne permet pas d'utiliser du câble à paires torsadées, le seul support physique disponible est donc la fibre optique. Le hub choisi en question b. ne possédant pas de ports d'entrée/sortie ST ou SC, il faut se procurer un transceiver 100BaseTX/100BaseFX à chaque extrémité de chacune des quatre liaisons, ce qui en fait de plus une solution très coûteuse. Une telle solution ne serait pas mise en place dans un cas réel.

La deuxième solution (*Fig. 7.48. (2a)*) propose de créer un second réseau Fast Ethernet autour d'un nouveau switch dans le service de gestion des commandes, puis d'interconnecter les deux réseaux locaux constitués. De même que pour la question précédente, le seul support utilisable est la fibre optique, nécessitant un transceiver à chacune de ses extrémités. Cette

structure est réaliste, elle est fréquemment rencontrée dans une telle situation.

La solution la plus complète techniquement est une variante de l'architecture *(2)*. Les deux réseaux locaux ne sont plus interconnectés directement, mais par l'intermédiaire d'un élément d'électronique active (*Fig. 7.48. (2b)*). Le matériel le plus adapté à ce rôle est un switch, qui permet de segmenter les domaines de collisions et ainsi de limiter les transmissions de trames Ethernet entre les deux hubs. Le support de transmission utilisé est fonction de l'emplacement physique du switch : si la longueur des liaisons entre ce dernier et les hubs des deux services n'excède pas 100 mètres, il est possible de choisir le câble à paires torsadées de Catégorie 5 ou la fibre optique. Cette architecture est de plus parfaitement évolutive : il est particulièrement simple d'ajouter une connexion avec un troisième réseau par exemple, ceci de manière homogène.

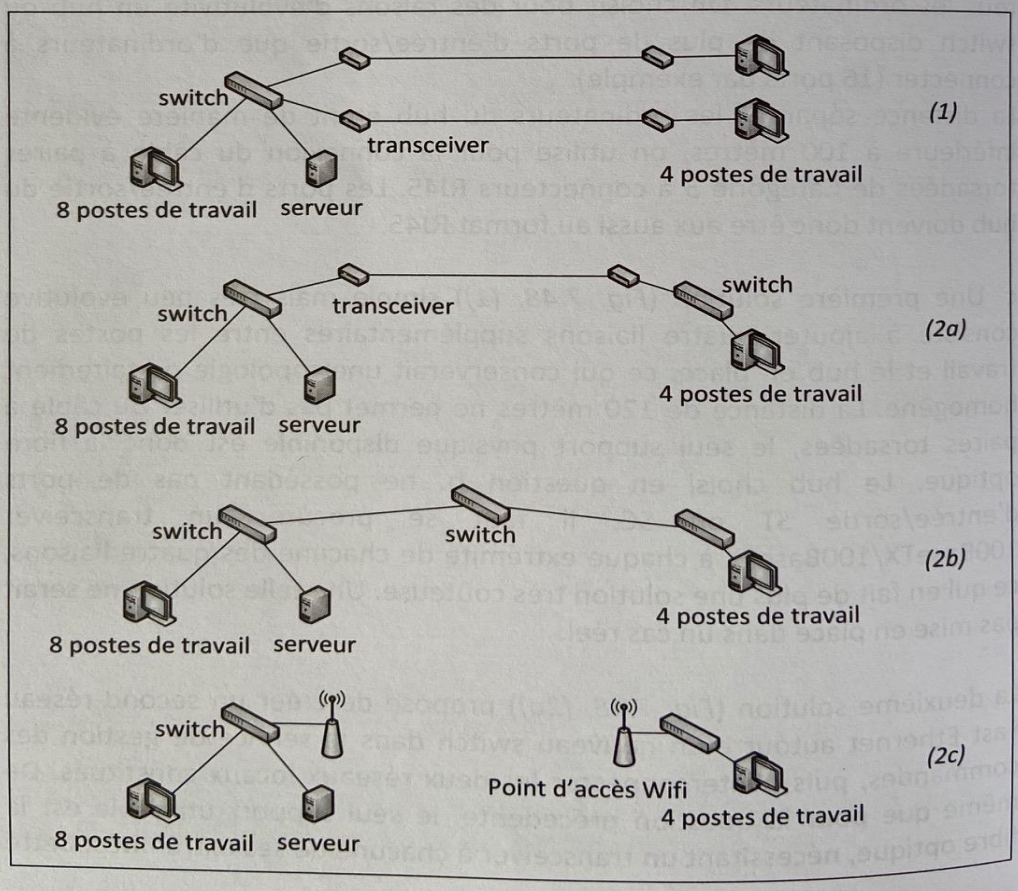

Fig. 7.48. Solutions envisageables

La troisième solution (*Fig. 7.48. (3)*) est proche de la deuxième : elle consiste à remplacer la liaison optique par une liaison sans fil (possible car la distance est inférieure à 200 m). Il suffit de remplacer dans la figure *Fig. 7.48. (2a)* les transceivers par des points d'accès Wifi jouant le rôle de pont 802.3u/802.11. On pourra opter pour la norme 802.11b ou 802.11g de manière à rapprocher au mieux le débit de la liaison inter-bâtiments de celui du réseau du service administratif.

d. Le réseau en place dans le local de stockage est un réseau *Token Ring*, conforme à la norme IEEE 802.5. Celui construit dans les questions a. à c. est une architecture Fast Ethernet, se référant à la norme 802.3u. L'élément qui permet d'interconnecter deux architectures de normes différentes est un pont. Supposons que c'est la solution *(3)* ci-dessus qui a été mise en place : on utilisera alors un pont 802.3u/802.5 entre le switch et un MAU du réseau *Token Ring*.

e. Dans notre cas, le serveur de prise de commandes est connecté d'une part à Internet, d'autre part au réseau local créé en question a. Cette structure peut être source d'accès indésirables ou de piratages sur le réseau local interne par des individus extérieurs à l'entreprise. Le pare-feu (firewall) est un élément qui permet de séparer physiquement deux parties d'un réseau par l'emploi de deux interfaces réseau et d'une passerelle applicative gérant les communications entre celles-ci. Il est particulièrement intéressant ici de ne pas laisser les personnes connectées au serveur via Internet accéder aux autres ordinateurs du réseau. Le pare-feu sera donc placé entre le serveur et le reste du réseau (*Fig. 7.49.*). Une solution à moindre coût pourrait être proposée, en plaçant le pare-feu directement sur le serveur, mais il semble judicieux pour accentuer la sécurité de répartir les rôles entre deux entités distinctes.

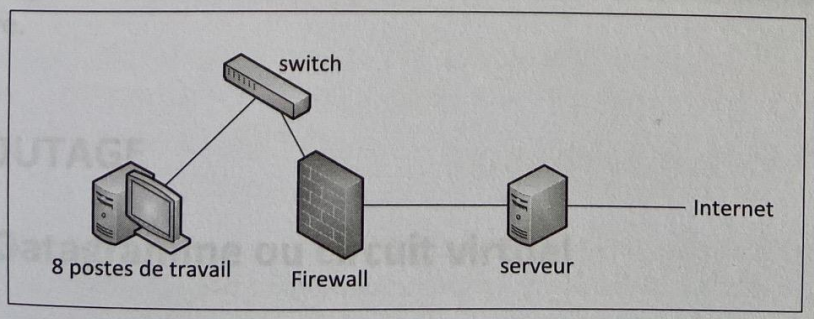

Fig. 7.49. Utilisation d'un pare-feu

Référence : *Bertrand Petit, « Architecture des réseaux : cours et exercices corrigés », Ellipses, 2017*