**Etude de la norme wifi 802.11**

***Un réseau Wifi bien sécurisé est aussi un réseau bien supervisé.***

**1.1 Masquer le SSID**

Il est parfois conseillé de masquer le SSID du réseau sans ﬁl. Un passant équipé d’un matériel Wifi classique ne saura pas qu’un réseau sans ﬁl se trouve à proximité ou en tout cas ne saura pas s’y associer facilement. Toutefois, il ne s’agit que d’une protection très faible, car il suffit de sniffer les ondes radio au moment où un utilisateur légitime se connecte : le SSID se trouve alors en clair dans sa requête d’association. En outre, chaque utilisateur légitime devra saisir manuellement le SSID du réseau sur son ordinateur. Bref, cette mesure apporte plus d’inconvénients que d’intérêts.

**1.2 Les VLAN**

Si les AP le permettent (ou les commutateurs auxquels ils sont reliés), il est bon d’associer le traﬁc sans ﬁl à un VLAN particulier. Ceci facilitera par la suite la maintenance et l’administration du réseau car tout le traﬁc provenant du réseau sans

ﬁl sera clairement identiﬁé.

En outre, certains AP peuvent associer un utilisateur donné à un VLAN particulier au moment de l’identiﬁcation (grâce au protocole RADIUS que nous étudierons au chapitre 10). Par exemple, lorsqu’un commercial se connecte au réseau sans ﬁl, il peut automatiquement être associé au VLAN numéro 10 qui lui donne accès aux serveurs généraux de l’entreprise ainsi qu’à des serveurs spéciﬁques aux commerciaux. Si un comptable se connecte, il peut être associé au VLAN numéro 20 qui lui donne accès aux serveurs généraux et aux serveurs réservés aux comptables. Enﬁn, si un simple visiteur se connecte, il peut être associé au VLAN numéro 30, lui donnant uniquement un accès limité et contrôlé à Internet.

Différentes politiques de qualité de service (QoS) peuvent être mises en œuvre sur les différents VLAN : un visiteur n’aura droit qu’à une très faible bande passante, alors que les commerciaux en auront suffisamment pour participer, par exemple, à des vidéoconférences.

**2 La solution VPN**

Des tunnels sécurisés Pour permettre aux employés d’accéder tout de même au réseau de l’entreprise lorsque le réseau sans ﬁl est isolé comme nous venons de le voir, il est possible de mettre en place un Réseau Privé Virtuel (RPV), plus connu sous le nom de Virtual Private Network (VPN). Cela consiste à mettre en place un serveur VPN entre les AP et le réseau local. Il existe même des AP qui intègrent un serveur VPN, par exemple le CN1050 de la société Colubris Networks. Le serveur VPN permet aux employés de créer de « tunnels » de communication sécurisés, établis au niveau des couches 2 (L2TP) ou 3 (PPTP, IP Sec...), voire dans des couches supérieures (SSH, SSL...).

Un employé commence par se connecter au réseau sans ﬁl.

À ce stade, il n’a pas encore accès au réseau local. Puis il exécute un logiciel (appelé le « client VPN ») qui établit une connexion sécurisée avec le serveur VPN, après identiﬁcation de l’utilisateur. Par la suite, l’employé a accès au réseau de l’entreprise au travers du tunnel VPN, comme s’il était connecté directement au réseau ﬁlaire. En outre, l’ensemble de son traﬁc est crypté entre son poste et le serveur VPN (ﬁg. 6.9).

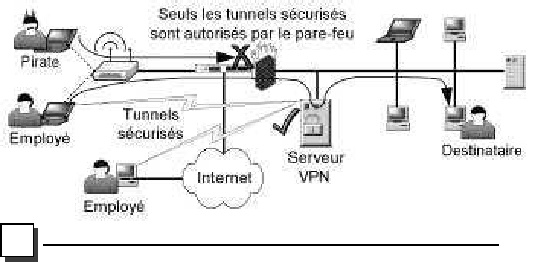
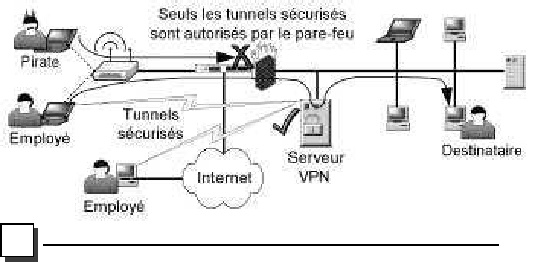
Autre avantage, on peut éventuellement rendre le serveur VPN accessible depuis

Internet et permettre ainsi aux employés de se connecter au réseau de l’entreprise

Pendant leurs déplacements (par exemple s’ils se connectent à des hotspots) ou depuis leur domicile. De nombreuses sociétés possèdent déjà un serveur VPN pour cet usage,

Ce qui évite d’avoir à en mettre un nouveau en place.

***Représentation de la solution VPN :***



Définition :

Un AP est : un matériel périphérique ou un ordinateur avec un logiciel, qui agit comme un concentrateur de communication pour les utilisateurs d'un dispositif sans fil. Cette appareil permet de se connecter à un câble LAN.