

FICHE 33 : Adresse MAC, adresse IP, masque réseau, port, pare-feu, VPN

I. Adresse physique : adresse MAC (Media Access Control) :

Une **adresse MAC** est affectée à un périphérique réseau Ethernet, c'est comme un numéro de série, il est donc unique au monde. Chaque constructeur de cartes réseau se voit attribuer par l'OUI (Organizationally Unique Identifier) une plage d'adresses qu'il affecte aux différentes **cartes réseau**.

Voici un exemple **d'adresse MAC** : « 00:19:7E:49:5E:96 ». Les trois premiers octets (00:19:7E) désignent le constructeur, les trois derniers octets (49:5E:96) sont les identifiants uniques de la carte donnés par le constructeur.

Il vient en complément de l'adresse IP qui, elle, est attribuée par le fournisseur d'accès ou par l'administrateur du réseau.

II. Adresse IP :

Une adresse IP est le numéro unique d'un ordinateur ou d'une machine sur un réseau qui lui permet de communiquer sur ce réseau. Deux postes ne peuvent pas avoir la même adresse IP sur un même réseau ; ce serait comme si deux personnes avaient le même nom et la même adresse postale.

Cette adresse IP est liée à la carte réseau de l'ordinateur (son adresse MAC). Il peut y avoir des postes ayant la même adresse IP sur différents réseaux, mais en aucune façon sur le même réseau.

Exemple : Un ordinateur a une adresse IP 190.12.24.56. À quoi cette adresse correspond-elle ?

190.12.24.56 est l'adresse IP (Internet Protocol), il est codé sur 4 octets (32 bits) comme défini dans la version 4 de l'Internet Protocol. La version IP V6 codée sur 128 bits est en déploiement et permettra de faire face à la saturation du nombre d'adresses IP nécessaires.

Une partie de l'adresse IP définit l'adresse du réseau et l'autre partie définit l'adresse de l'hôte dans le réseau.

Il existe 3 classes d'adresses IP

	Adresse réseau	Adresse hôte		
Classe A	Octet 4	Octet 3	Octet 2	Octet 1
Classe B	Octet 4	Octet 3	Octet 2	Octet 1
Classe C	Octet 4	Octet 3	Octet 2	Octet 1

La **classe A** permet de créer **peu de réseaux**, mais avec **beaucoup d'hôtes** dans chaque réseau. La **classe C fait l'inverse**.

	Adresse réseau		Adresse hôte
Classe A	0	+ 7 bits = 126 réseaux	24 bits = 16 777 214 hôtes
Classe B	10	+ 14 bits = 16 383 réseaux	16 bits = 65 534 hôtes
Classe C	110	+ 21 bits = 2 097 161 réseaux	8 bits = 254 hôtes

Il y a des adresses auxquelles on n'applique pas de numéro d'hôte :

- l'adresse d'hôte = 0 (exemple : 194.118.21.0) est réservée à l'identification du réseau ;
- l'adresse d'hôte = 255 qui a tous ses bits à 1 (exemple : 194.118.21.255).



III. Le masque de réseau

Le masque de réseau est un ensemble de 4 octets qui permet de différencier l'adresse du réseau et l'adresse de l'hôte.

Adresse IP	194.118.21.12	Adresse IP de classe B d'un poste sur le réseau 194.118 avec comme n° d'hôte : 21.12
Masque de réseau	255.255.0.0	

Adresse IP	194.118.21.12	Adresse IP de classe C d'un poste sur le réseau 194.118.21 avec comme n° d'hôte : 12
Masque de réseau	255.255.255.0	

IV. La notion de port

Le port correspond à la couche de transport du modèle OSI. La notion de port logiciel permet, lorsque l'ordinateur est identifié par l'adresse IP, de distinguer à quelle application logiciel un paquet de donnée est destiné (le navigateur web, le jeu en ligne, le logiciel de messagerie mail...). Un port est distingué par son numéro [document 8].

POP3 : port 110

HTTP : port 80

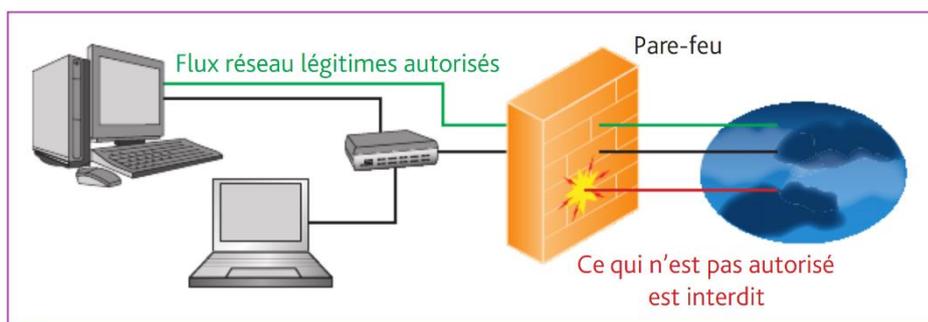
FTP : port 21

V. Le pare-feu

Le pare-feu (ou firewall en anglais) est un équipement de sécurité (logiciel ou matériel) entre plusieurs réseaux informatiques. Il filtre les paquets en transit en suivant des règles de filtrage qui protègent et régulent l'accès aux ressources réseau parfois sensibles.

En fonction de la politique de sécurité de l'administrateur du réseau (origine, destination des paquets...), il autorise ou non les informations à le traverser [document 9].

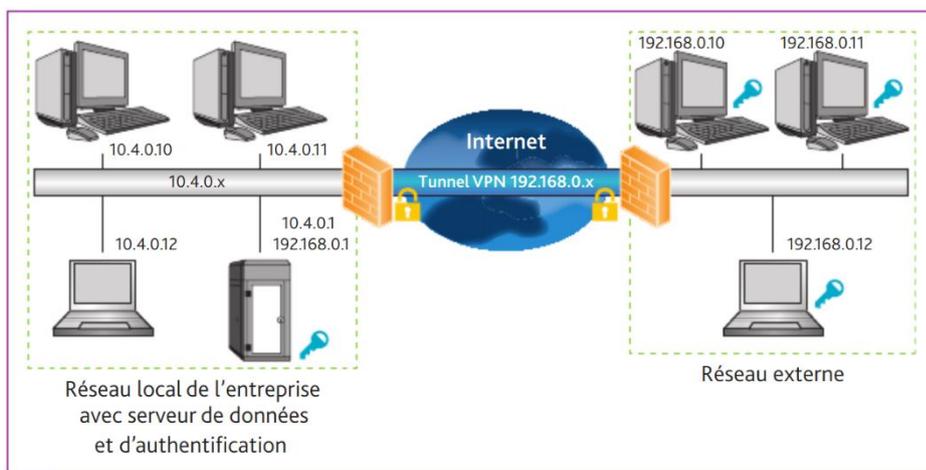
8 Numéros de port.



9 Principe du pare-feu.

VI. Le VPN

Un réseau VPN est un protocole qui permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre d'un tunnel. Les utilisateurs ont l'impression de se connecter sur un poste (ou machine) du LAN alors qu'en réalité ce poste (ou machine) peut être très éloigné et oblige donc à passer par le WAN [document 10].



10 Principe du VPN.

