

ADRESSE IP - CLASSES DE RESEAU

CLASSE A :

Limite de la classe A

Calcul du 1^{er} octet

1^{er} bit du 1^{er} octet à 0

0000 0000 à 0111 1111 ► 01111111 == 127

De 0 à 127 mais 0 est interdit et 127 est réservé (localhost)

Donc de 1 à 126

Adressage : **1.X.X.X à 126.X.X.X**

Masque de sous réseau

Par défaut **255.0.0.0**

@IP

10.0.0.1

Masque

255.0.0.0

(255 = 1111 1111)

AND

10.0.0.0

Numéro de réseau

En binaire **1 AND X donne X**

0 AND X donne 0

Règle Importante
à 0 ou à 1

Dans le numéro de réseau, on ne peut pas avoir tous les bits

CLASSE B

Limite de la classe B

Calcul du 1^{er} octet

Les **2** premiers bits du 1^{er} octet sont **10**

1000 0000 à 10111111

Adressage : **128.X.X.X à 191.X.X.X**

Masque de sous réseau

Par défaut **255.255.0.0**

CLASSE C

Limite de la classe C Calcul du 1^{er} octet

Les **3** premiers bits du 1^{er} octet sont **110**

11000000 à **110**11111

Adressage : 190.X.X.X à 223.X.X.X

Masque de sous réseau

Par défaut 255.255.255.0

CLASSE D - MULTIDIFFUSION - MULTICAST

Limite de la classe D Calcul du 1^{er} octet

Les **4** premiers bits du 1^{er} octet sont **1110**

11100000 à **1110**1111

Adressage : 224.X.X.X à 239.X.X.X

CLASSE E - INTERDIT

Limite de la classe E Calcul du 1^{er} octet

Les **4** premiers bits du 1^{er} octet sont **1111**

11110000 à **1111**1111

Adressage : 240.X.X.X à 255.X.X.X

NOTATION CIDR - CLASSLESS INTERDOMAIN ROUTING

192.168.0.1
10.0.0.1

Masque 255.255.0.0
Masque 255.0.0.0

Notation CIDR
Notation CIDR

192.168.0.1/16
10.0.0.1/8

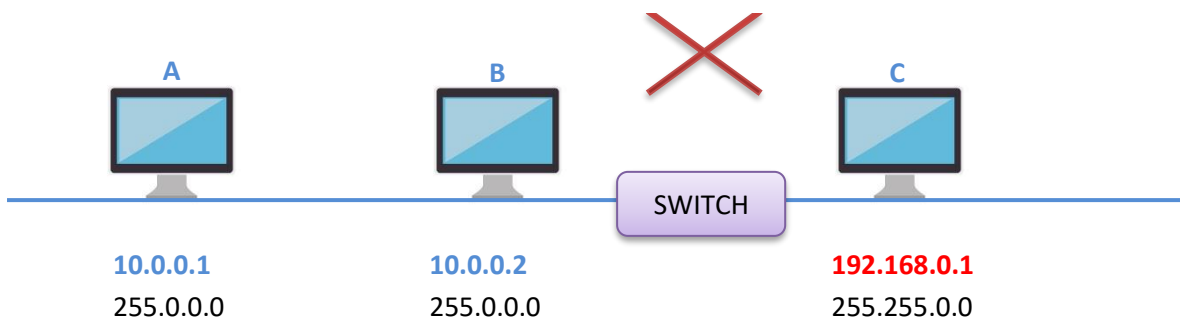


10.0.0.1
255.0.0.0

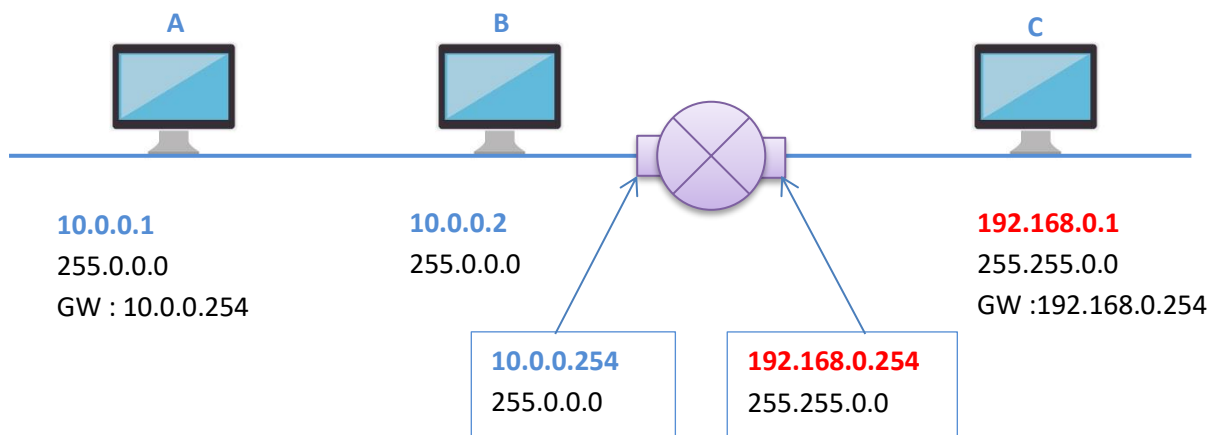


192.168.0.1
255.255.0.0

Communication Impossible



A et B peuvent communiquer car ils sont sur le même réseau mais ne peuvent pas communiquer avec C qui est sur un autre réseau.



1 Routeur a au moins 2 interfaces réseau (cartes réseaux) pour joindre 2 réseaux

1 @IP par carte.

On doit définir une passerelle par défaut ► **Passerelle == Routeur**

Par convention l'@IP de la passerelle est X.X.X.**254**

En pratique :

A Tente de communiquer avec C
Il ne le voit pas dans son réseau local
Il invoque alors sa passerelle par défaut 10.0.0.254
Qui elle peut communiquer avec le 2nd réseau

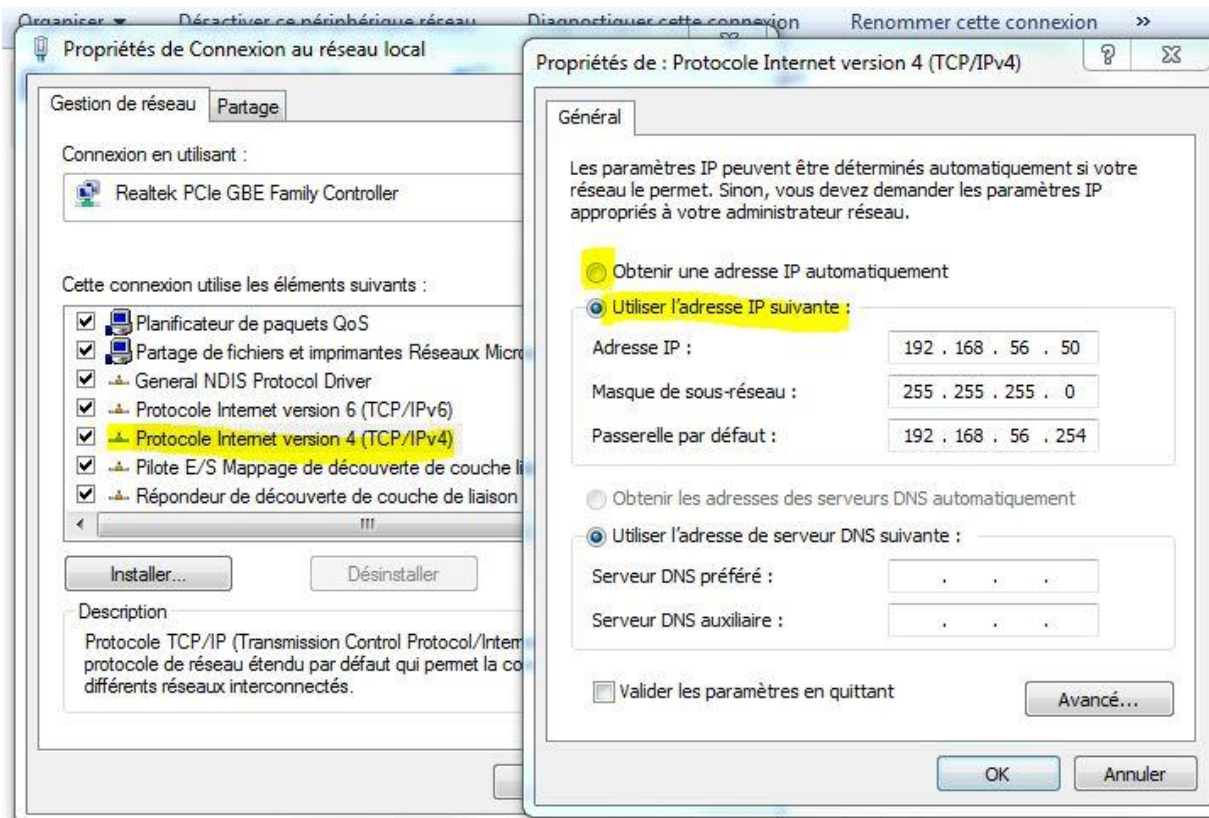
Panneau de configuration

Centre réseau et partage

Modifier les paramètres de la carte

On trouve une icône par carte réseau

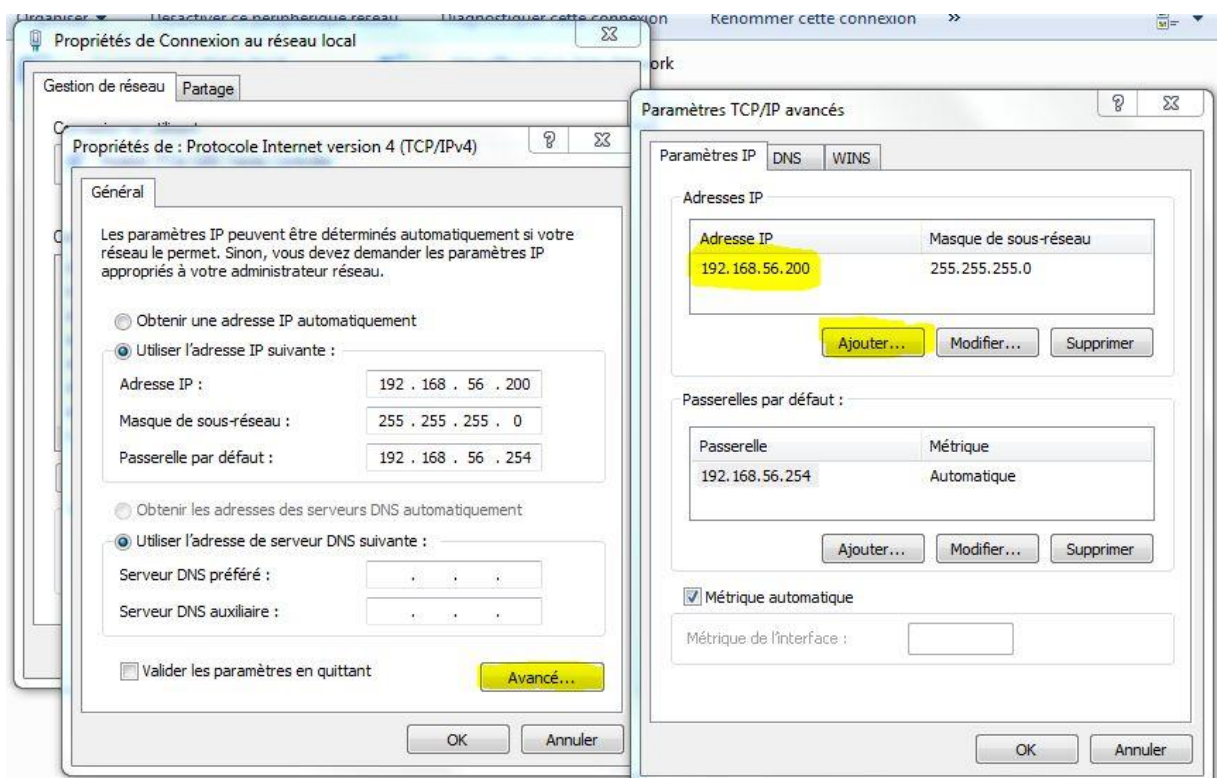
Bouton Droit Propriété



Ipconfig /all pour avoir un maximum d'informations

On peut configure plusieurs @IP par carte /PC en allant dans avancé puis ajouter ..

Cas du routeur :



ADRESSES INTERNES

- 10.0.0.0/8	Classe A			
- 192.168.0.0/16	Classe B			
		Sous-Réseau	192.168.1.0/24	Classe C
		Sous-Réseau	192.168.2.0/24	Classe C
- 172.16.0.0/12	16			
16 en binaire	000 1 0000			
Masque	0000 1111			
Max avec masque de 12	000 1 1111	31	de 172.16.X.X à 172.31.X.X	

COMMANDE PING

Ping 192.168.1.1

On a pinger une @IP mais ce sont avant tout les @MAC des cartes qui communiquent
Les @MAC sont sous la forme de 6 octets codés en hexadécimal

The image shows a Wireshark packet capture of a ping command. The top pane displays a list of packets, with the selected packet (No. 4) showing an ICMP Echo (ping) request from 192.168.1.1 to 192.168.1.1. The bottom pane shows the packet details, including the Ethernet II header and the Internet Protocol Version 4 header. A red arrow points from the MAC address b8:26:6c:b7:ee:9e in the Ethernet II header to the corresponding MAC address in the Windows PowerShell output.

Administrateur : Windows PowerShell

```
PS C:\Users\Mini> ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Mini>
```

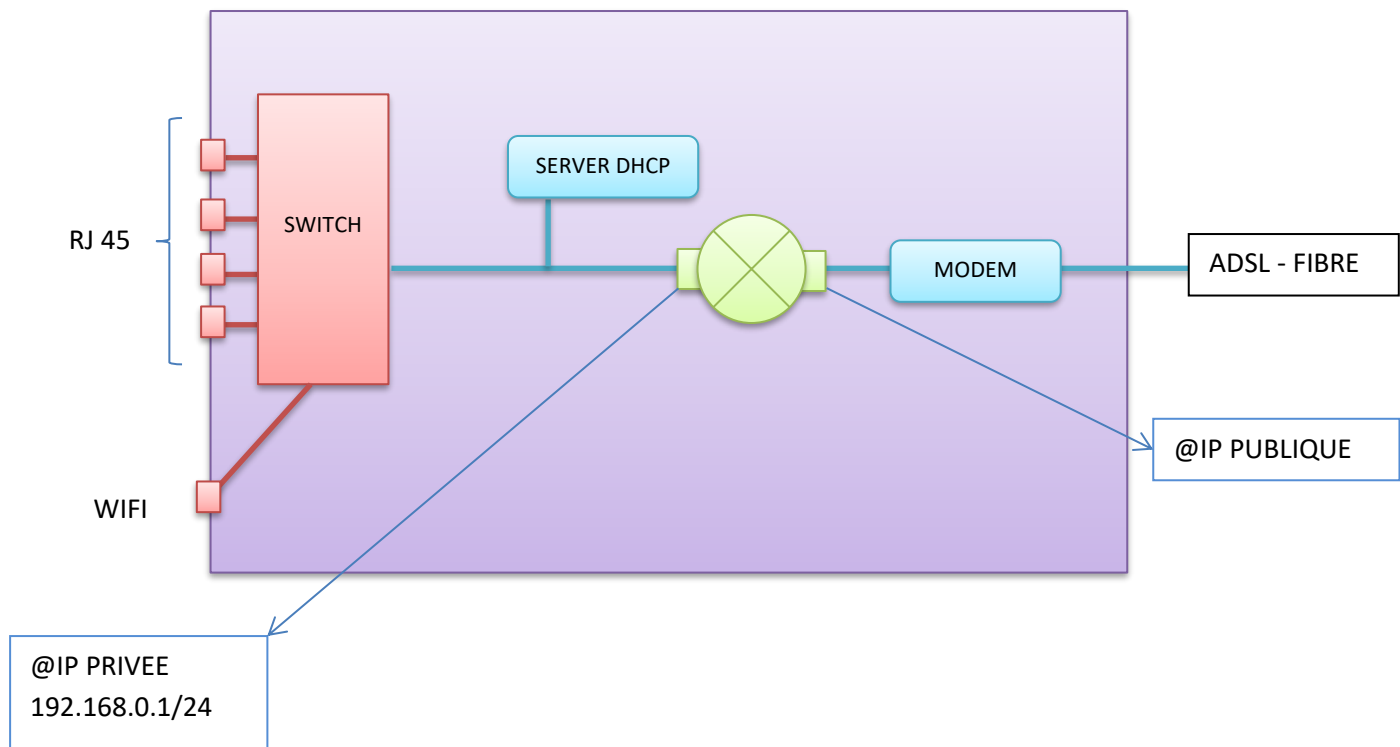
```
PS C:\Users\Mini> ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : PC1
Suffixe DNS principal . . . . . : 
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: home

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . . . : home
    Description. . . . . : Realtek PCIe GBE Family Controller
    Adresse physique . . . . . : E8-39-35-56-D0-30
    DHCP activé . . . . . : Oui
    Configuration automatique activée. . . . . : Oui
    Adresse IPv6. . . . . : 2a01:cb1d:27e:1500:2d84:ae85:9bcc:c774c
    Adresse IPv6 temporaire . . . . . : 2a01:cb1d:27e:1500:14f0:490:843:7fac
    Adresse IPv6 de liaison locale. . . . . : fe80::2d84:ae85:9bcc:c774x13<préféré>
    Adresse IPv4. . . . . : 192.168.1.9<préféré>
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mardi 22 novembre 2016 12:17:49
    Bail expirant. . . . . : mercredi 23 novembre 2016 12:17:48
    Passerelle par défaut. . . . . : fe80::ba26:6cff:feb7:ee9ex13
    192.168.1.1
    Serveur DHCP . . . . . : 192.168.1.1
    IAID DHCPv6 . . . . . : 272423211
    DUID de client DHCPv6. . . . . : 00-01-00-01-16-F6-DE-03-E8-39-35-56-D0-30
    Serveurs DNS. . . . . : fe80::ba26:6cff:feb7:ee9ex13
    192.168.1.1
```

LES BOX INTERNET



SERVEUR DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL

Donner une configuration IP à une ou plusieurs machines sur le réseau.

Le DHCP est installé sous Windows avec Windows SERVER 2008 -2012 - 2016

Le serveur DHCP gère une étendue == une plage d'@IP

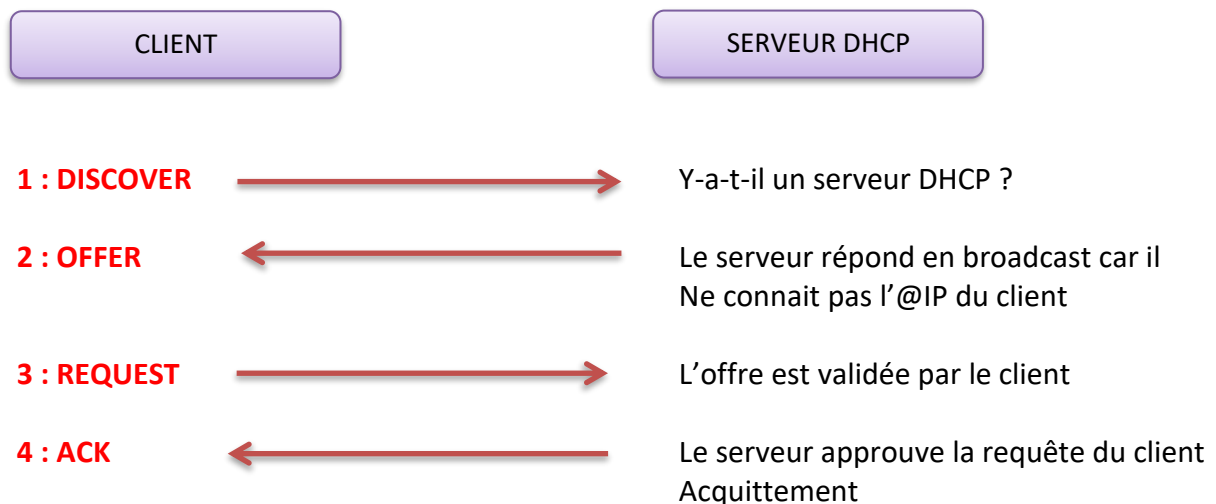
SERVER DHCP

- Etendue
- Plage d'@IP
- Options
- Passerelle par défaut
- @IP du DNS

1 Poste sans @IP peut quand même faire de la diffusion (broadcast) avec une @IP de type 255.255.255.255

Le dialogue DHCP fonctionne avec des messages de diffusion (broadcast).

4 échanges entre le client et le serveur



Le client possède alors une @IP avec un **bail**. Par défaut sous Windows le bail a une durée de 8 jours.

Au bout de 4 jours, le client renvoie les 2 dernières trames en accès direct (pas en broadcast) car il connaît l'@IP du serveur. S'il y a acquittement le client reprend un bail de 8 jours.

S'il n'y a pas de réponse au bout des 7 jours, le client renvoie les 4 trames en broadcast pour retrouver par exemple la nouvelle @IP du serveur DHCP. (On a changé par ex. le serveur DHCP entre temps)

Etendue :

Tous les serveurs (DHCP DNS), les routeurs et les imprimantes sont en adresses IP Fixe. Imprimantes également car c'est un serveur d'impression.

Les postes clients peuvent être en Fixe ou en Dynamique

WireSharck Capture de dialogue DHCP

Ipconfig /release

Ipconfig /renew

The screenshot displays a Wireshark network capture of a DHCP transaction. The packet list on the left shows several frames, with frame 6 (342 bytes) selected, which is a DHCP Discover packet. The packet details pane on the right shows the structure of this packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Bootstrap Protocol (Discover). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Overlaid on the Wireshark window is a Windows command prompt window titled "Administrateur: C:\Windows\system32\cmd.exe". It shows the execution of the command `C:\Users\Mini>ipconfig /renew`. The output of the command is as follows:

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . :

C:\Users\Mini>ipconfig /renew

Configuration IP de Windows

Une erreur s'est produite lors de la libération de l'interface Loopback Pseudo-Interface 1 : Le fichier spécifié est introuvable.

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . : none
    Adresse IPv6. . . . . : 2a01:chid:27e:1500:2d04:ae85:9bcc:c774
    Adresse IPv6 temporaire. . . . . : 2a01:chid:27e:1500:14f0:490:843:7fac
    Adresse IPv6 de liaison locale. . . . : fe80::2d04:ae85:9bcc:c774%13
    Adresse IPv4. . . . . : 192.168.1.9
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : fe80::ba26:6cff:feb7:ee9e%13
    192.168.1.1

Carte Ethernet VirtualBox Host-Only Network :
    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::b932:28a6:18e1:8d9a%21
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Tunnel Connexion au réseau local* 9 :
    Statut du média. . . . . : Média déconnecté
```

Adressage Privé Internet Automatique APIPA

Si le client ne trouve pas de serveur DHCP, le client s'octroie une @IP dans ce réseau 169.254.0.0/16. Il ne pourra pas aller sur Internet et ne peut pas communiquer avec le reste du réseau.

Ipconfig /release

```
Suffixe DNS propre à la connexion. . . :  
C:\Users\Mimi>ipconfig  
Configuration IP de Windows  
  
Carte Ethernet Connexion au réseau local :  
Suffixe DNS propre à la connexion. . . : home  
Adresse IPv6. . . . . : 2a01:cb1d:27e:1500:2d84:ae85:9bcc:c774  
Adresse IPv6 temporaire . . . . . : 2a01:cb1d:27e:1500:14f0:490:843:7fac  
Adresse IPv6 de liaison locale. . . . : fe80::2d84:ae85:9bcc:c774%13  
Adresse d'autoconfiguration IPv4 . . . : 169.254.199.116  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . : fe80::ba26:6cff:feb7:ee9e%13  
  
Carte Ethernet VirtualBox Host-Only Network :
```

Menu Outils	Console DHCP
Protocole IPV4	Bt Droit Nouvelle étendue
@IP début et fin	192.168.255.100 à 192.168.255.150
CIDR et Masque	
Exclusions	Durée du bail
Options	Passerelle par défaut 192.168.255.1
DNS	
WINS (OLD compatibilité anciens systèmes)	
Activer	

SECURITE - PORTS

Pour identifier un poste, on a besoin d'une @IP. La trame Réseau a une @IP source et une @IP destination. Ceci permet de faire communiquer les machines.

Une fois arrivée dans la machine destinataire, ou est dirigé la trame (Server DNS, server DHCP ...)

Cet aiguillage se fait grâce aux ports.

@IP  N° de port TCP ou UDP

Liste des principaux Ports :

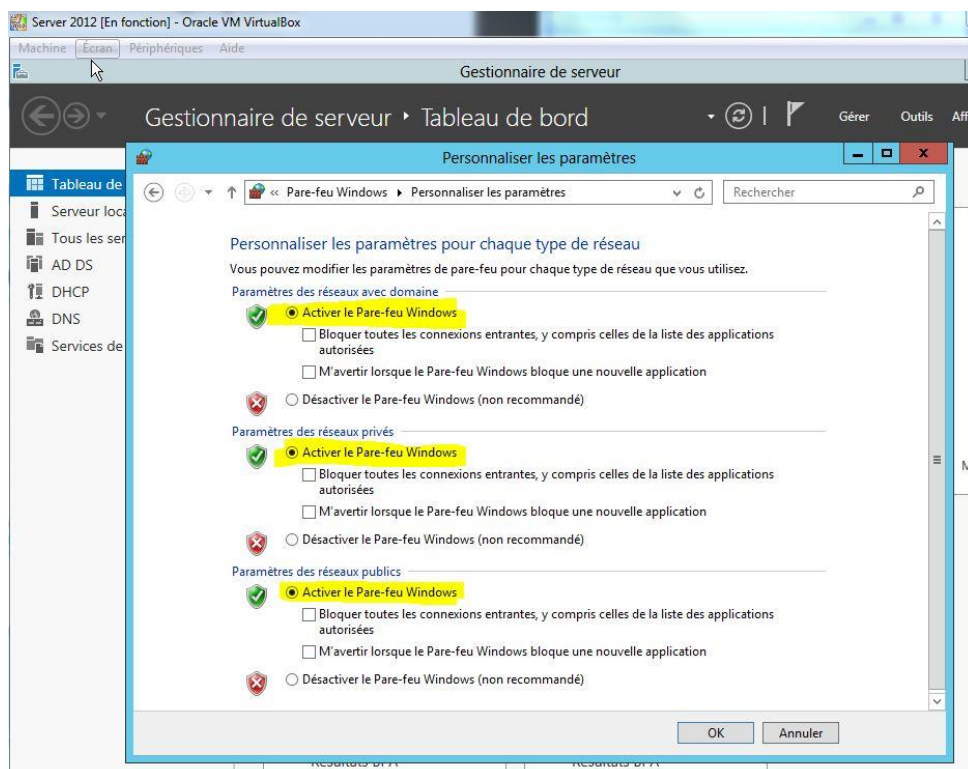
HTTP	TCP 80
HTTPS	TCP 443
SMTP	TCP 25
POP	110
DNS	TCP UDP 53

SECURITE - PARE FEU

Le pare Feu peut être matériel intégré dans une baie.

Le pare feu Logiciel est installé par défaut dans Windows.

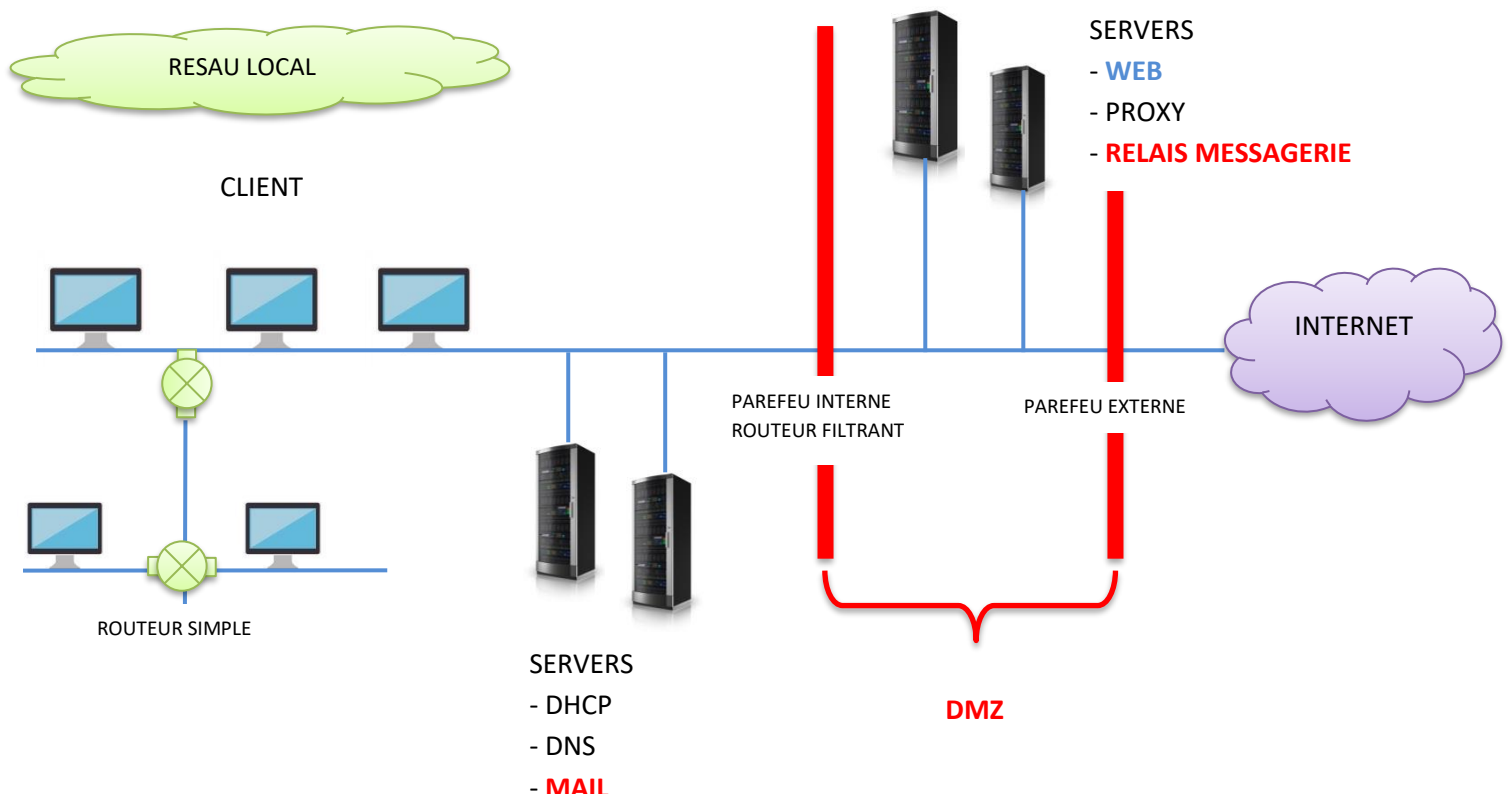
Réglages Panneau de Configuration. WIN + I



Dans les paramètres avancés

Règles de trafic entrant | sortant

DMZ



@IP Privé

- 10.0.0.0/8
- 192.168.1.0/24
- 172.16.0.0/12

@IP Publiques

Règle :

WEB HTTP :

< port TCP 80 Bloqué < port TCP 80 Ouvert
> Port TCP 21 Ouvert

Les requêtes entrantes depuis l'Internet pour consulter le site Web sont autorisées dans la DMZ mais pas dans le réseau Local.

Les développeurs peuvent faire les mises à jour du Site en FTP.

PROXY :

Les utilisateurs du réseau local ont accès au Proxy par le Parfeu Interne

ROUTEUR SIMPLE :

Aiguille une trame. Il connaît l'@IP de destination. Il connaît les différents chemins grâce à ses tables de routage. On parle de coût en optimisant le chemin le plus rapide.

ROUTEUR FILTRANT :

Filtre par rapport à :

- @IP source
- @IP Destination
- un numéro de port

PAREFEU :

+ Performant peut filtrer par rapport au service | Application
On va au-delà du contenu de la trame

TABLE DE ROUTAGE

Les routeurs possèdent des tables de routage.

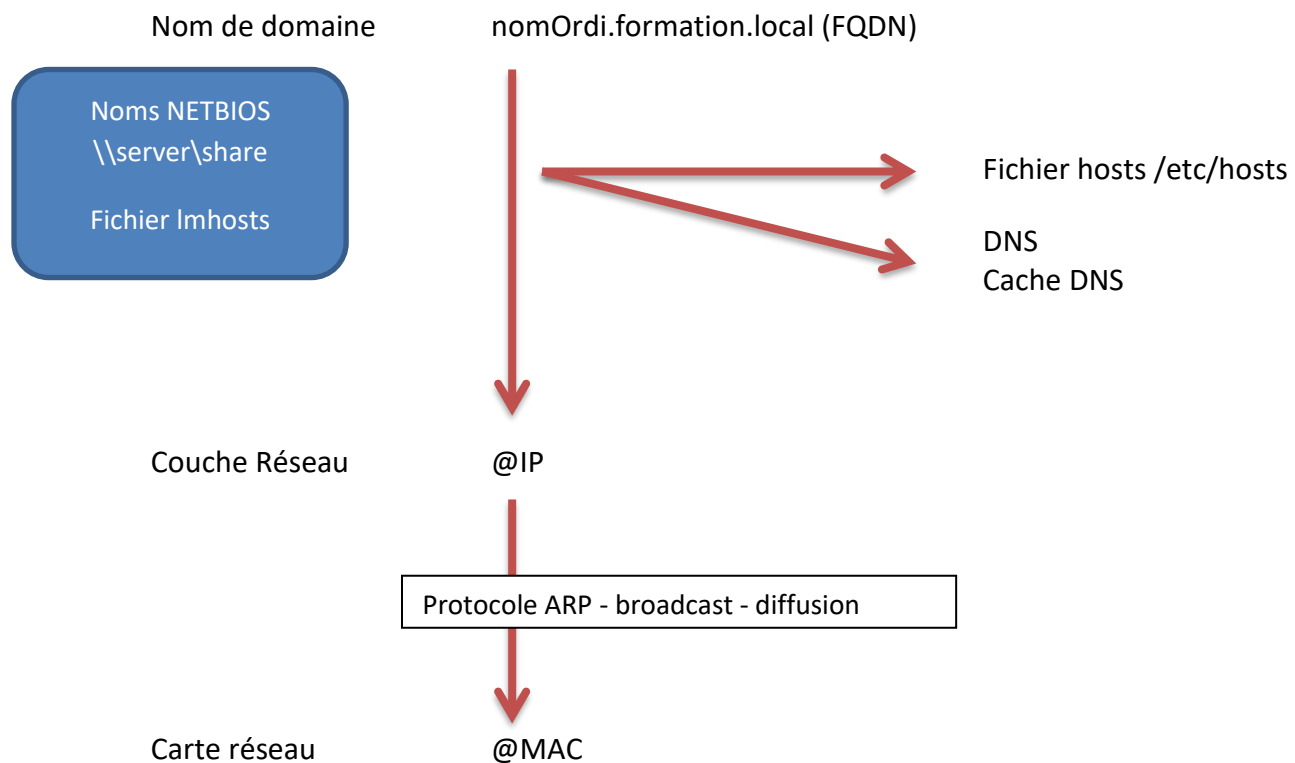
La table de routage peut être statique. L'administrateur doit renseigner sa table de routage.

Commandes

ROUTE PRINT

ROUTE ADD

DNS - DOMAIN NAME SERVICE



Au tout début on utilisait le fichier hosts /etc/hosts avec la liste des noms de machines et correspondance @IP. Il n'y avait que quelques centaines de noms (comme lmhosts) et chaque machine devait détenir ces fichiers.

C:\windows\system32\drivers\etc

Ipconfig /displaydns

Ipconfig /flushdns

Ipconfig /registerdns

Nom NETBIOS

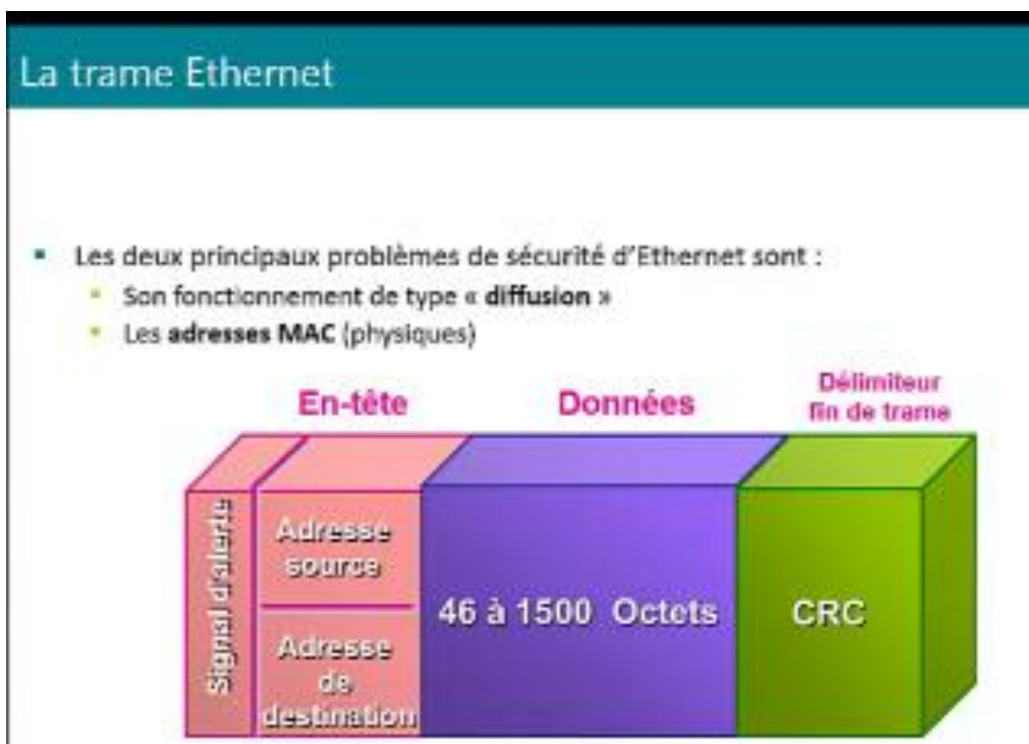
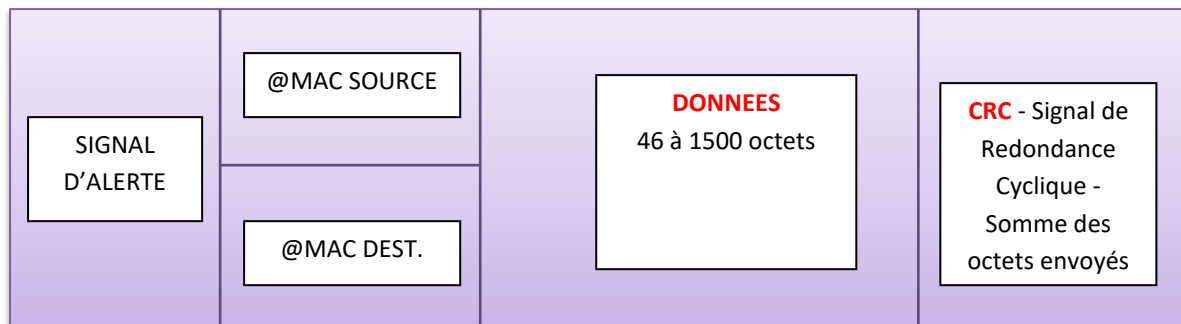
Le nom NETBIOS est le nom de l'ordinateur. Sous dos on peut saisir hostname.

WINS (Windows Internet Name Service) est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.

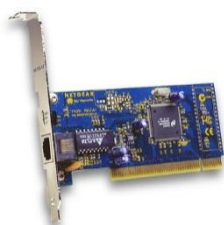
Depuis Windows 2000, Microsoft conseille à ses clients d'utiliser Active Directory (et le DNS Dynamique) plutôt que WINS.

En pratique, WINS est aux noms Netbios, ce que le DNS est au FQDN - un dépôt central d'informations (base de données), auquel un client voulant contacter un ordinateur sur le réseau peut envoyer des requêtes pour trouver l'adresse IP à joindre, plutôt que d'envoyer une requête globale (à tout le monde - broadcast -) pour demander l'adresse à contacter. Le système réduit alors le trafic global sur le réseau.

TRAME ETHERNET



Le signal d'alerte est un signal électronique envoyé par la carte pour informer l'envoi de la trame. Ce signal ne remonte pas dans WireSharck !



La carte 1 envoie la trame, calcule son CRC1 et l'envoie également.

La carte 2 réceptionne la trame, calcule le CRC2 de cette trame.

Si le CRC2 != CRC1 , la trame est rejetée.

Le protocole ARP met en relation les @MAC (physiques) et les @IP (logiques).

L'@MAC de diffusion (broadcast) contient 6 octets à 255 FF.FF.FF.FF.FF.FF

COMMANDES RESEAUX

Tracert www.google.fr

Tracert (tracert) est un autre vieil outil emprunté à Unix. Le chemin entre deux ordinateurs sur Internet n'est pas en ligne droite mais consiste en de nombreux segments ou "hops" d'un ordinateur intermédiaire à un autre. Tracert affiche chaque étape du chemin emprunté. Il peut être intéressant de voir jusqu'à quel point il est compliqué. Le temps pour chaque "hop" et l'adresse IP de chaque ordinateur intermédiaires sont affichés. Tracert affiche jusqu'à 30 "hops". Cela est particulièrement utile pour savoir si un segment particulier provoque une mauvaise connexion ou une lenteur. La commande peut s'écrire par exemple "tracert dell.com".

Pathping www.google.fr

Pathping va tout d'abord lister le nombre de "hops" nécessaires pour atteindre l'adresse que vous testez puis va envoyer plusieurs pings à chaque routeur entre vous et la destination. Après cela, la commande calcule les résultats basés sur les paquets renvoyés par chaque routeur. Comme pathping affiche la proportion de paquets perdus pour chaque routeur ou lien, vous pouvez déterminer quels routeurs ou sous-réseaux ont des problèmes de réseau. Notez que le processus complet peut prendre entre 5 et 10 minutes parce que beaucoup de pings sont envoyés. Cette commande dispose de plusieurs options pour modifier le processus. Vous pouvez voir ces options en tapant "pathping /?" dans l'invite de commande.

Netsat –an

Netstat affiche les connexions TCP actives et les ports sur lesquels l'ordinateur est en écoute, les statistiques ethernet, la table de routage IP ainsi que les statistiques pour les protocoles IP, ICMP, TCP et UDP. Elle dispose de nombreuses options pour afficher plusieurs propriétés du réseau et des connexions TCP. (Un point à noter : les options sont préfixée par un tiret et non pas un slash). Vous trouverez plus d'informations sur cette page. Vous pouvez par exemple utiliser Netstat pour déterminer si un spyware ou un ver a établi des connexions sans que vous ne le sachiez. La commande "netstat -a" affiche toutes les connexions. La commande "netstat -b" affiche les fichiers exécutables qui ont ouvert des connexions. Vous pouvez voir toutes les options et la syntaxe dans l'image ci-dessous.