La sécurité à travers les VLAN, VPN et le filtrage

DUT 2

ADMN RESEAUX

H. Moungla & Y. Grusson

Introduction

La protection et la sécurité des données échangées sur les réseaux publics et locaux doit être complétée par la maîtrise du trafic des informations qui les traversent.

Introduction

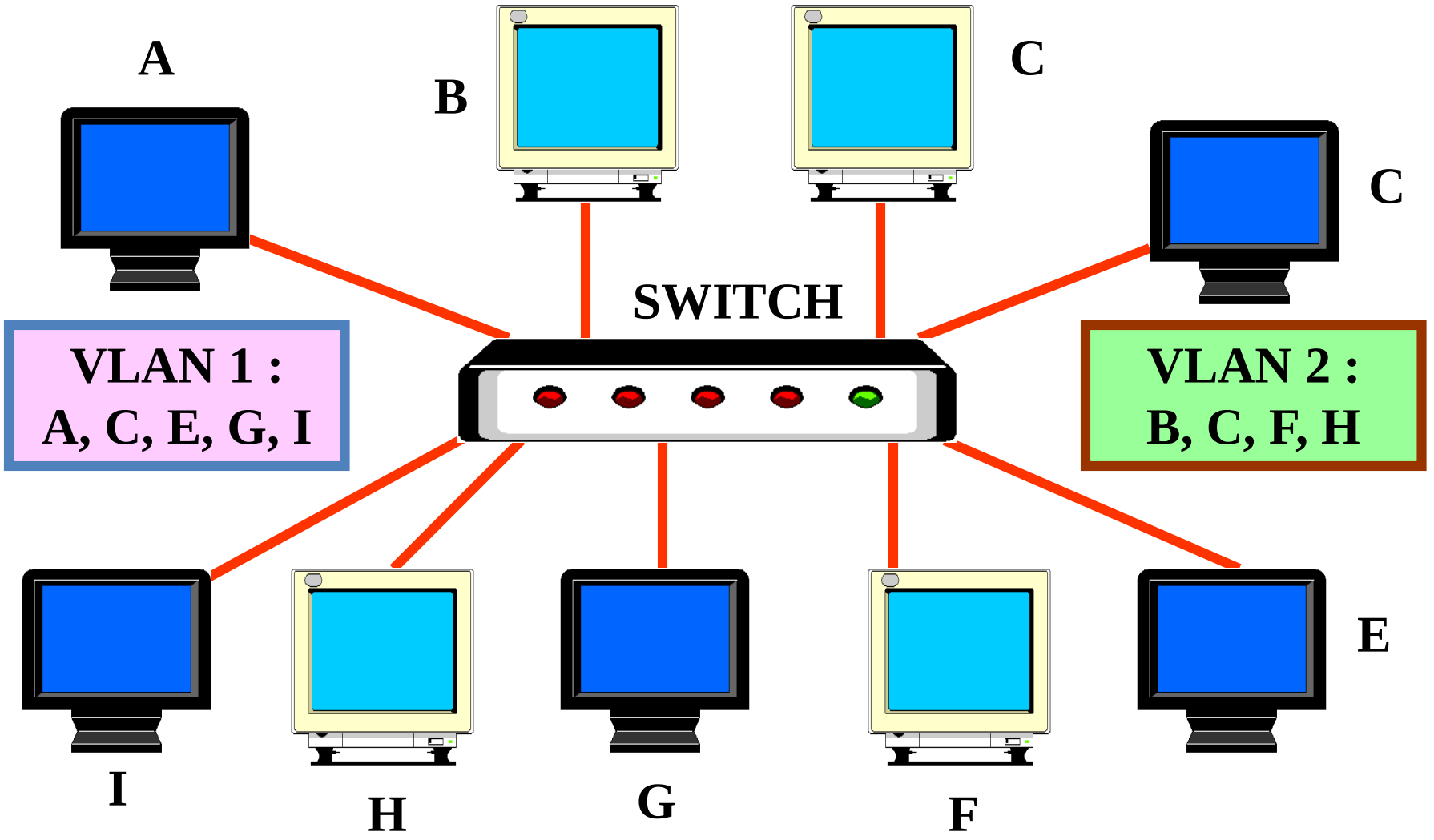
PLAN

- Le Virtual Local Area Network (VLAN)
- Le Virtual Private Network (VPN)
- Les techniques du filtrage
  - ✓ Le routage filtrant
  - ✓ Le pare-feu (Firewall)
  - ✓ Le serveur NAT (Network Adress Translation)
  - ✓ Le serveur Proxy
- Notion de "Zone Démilitarisée" (DMZ)

Le VLAN

- L'idée du VLAN est de regrouper des machines d'un réseau local et de limiter la diffusion des informations qu'entre les membres de ce groupe de machines.
- On parlera de réseau virtuel car les machines restent physiquement connectés aux autres machines.
- Le "dispatching" des trames est assuré par les appareils d'interconnexion (Switch en général).

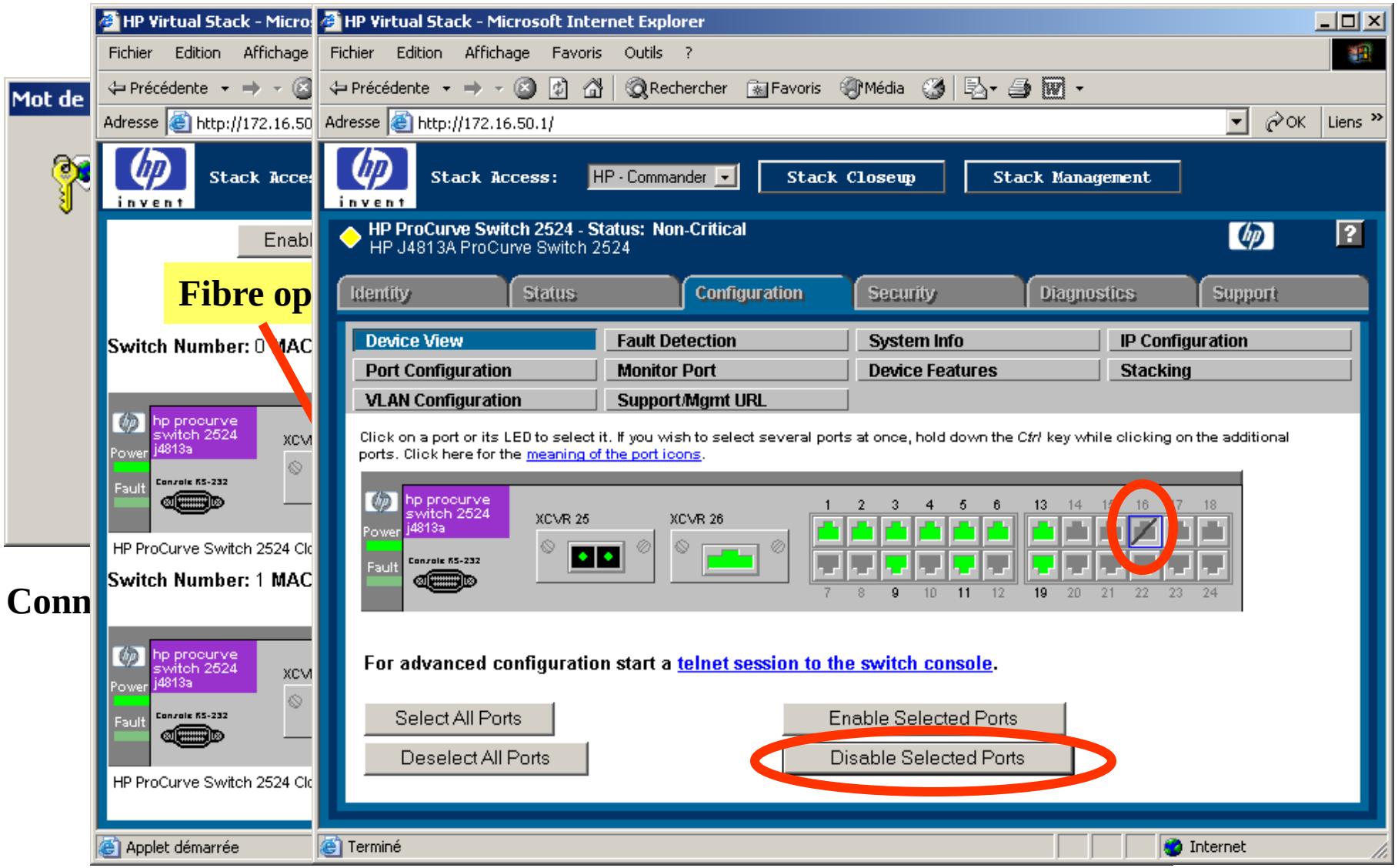
Le VLAN



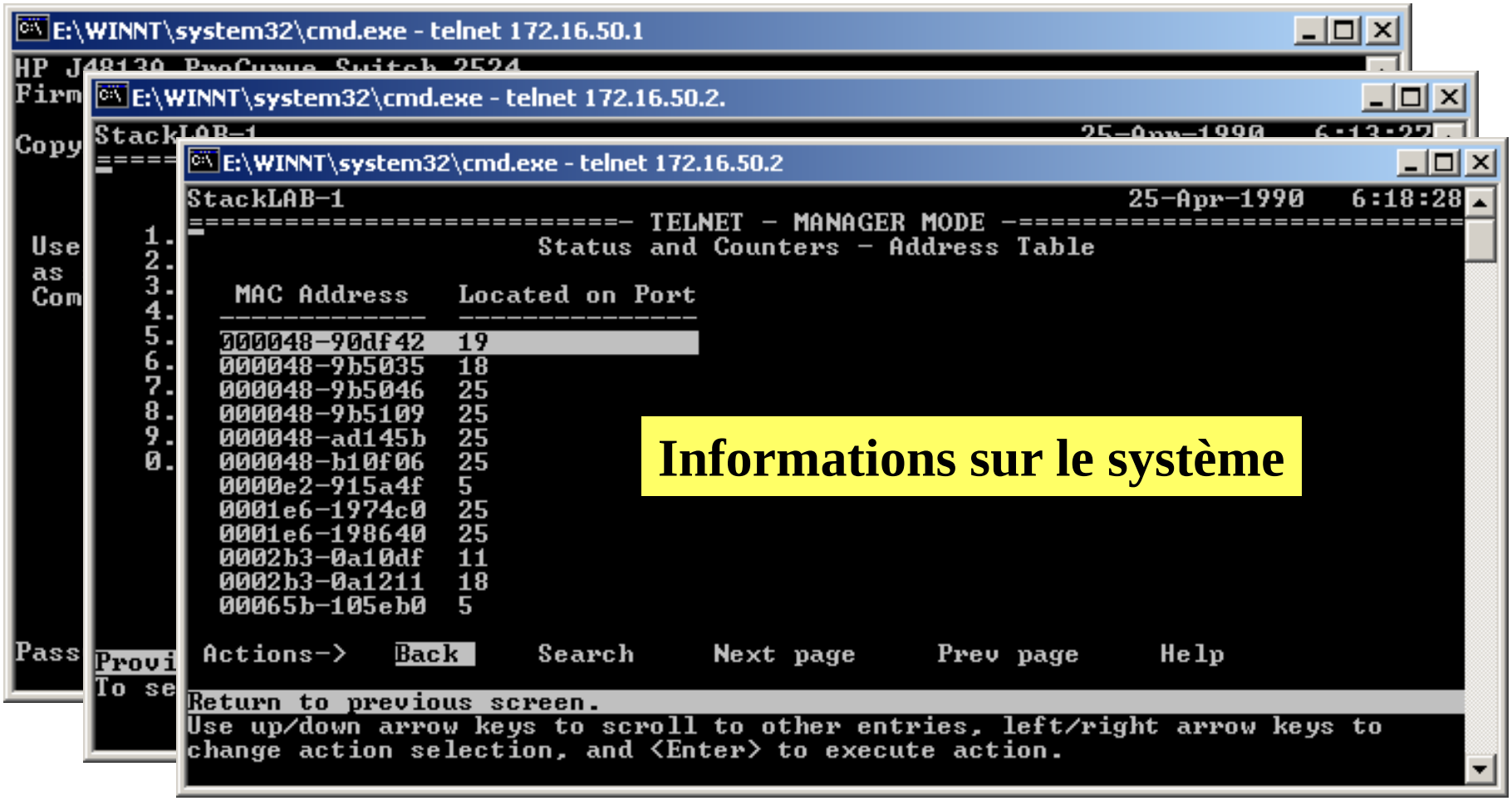
Le VLAN

- Le VLAN est défini par l'administrateur au niveau du commutateur qui doit être dans ce cas manageable en général à l'aide d'un navigateur Web et/ou un client Telnet.
- Exemple de configuration d'un Switch HP Procurve 2524

Le VLAN

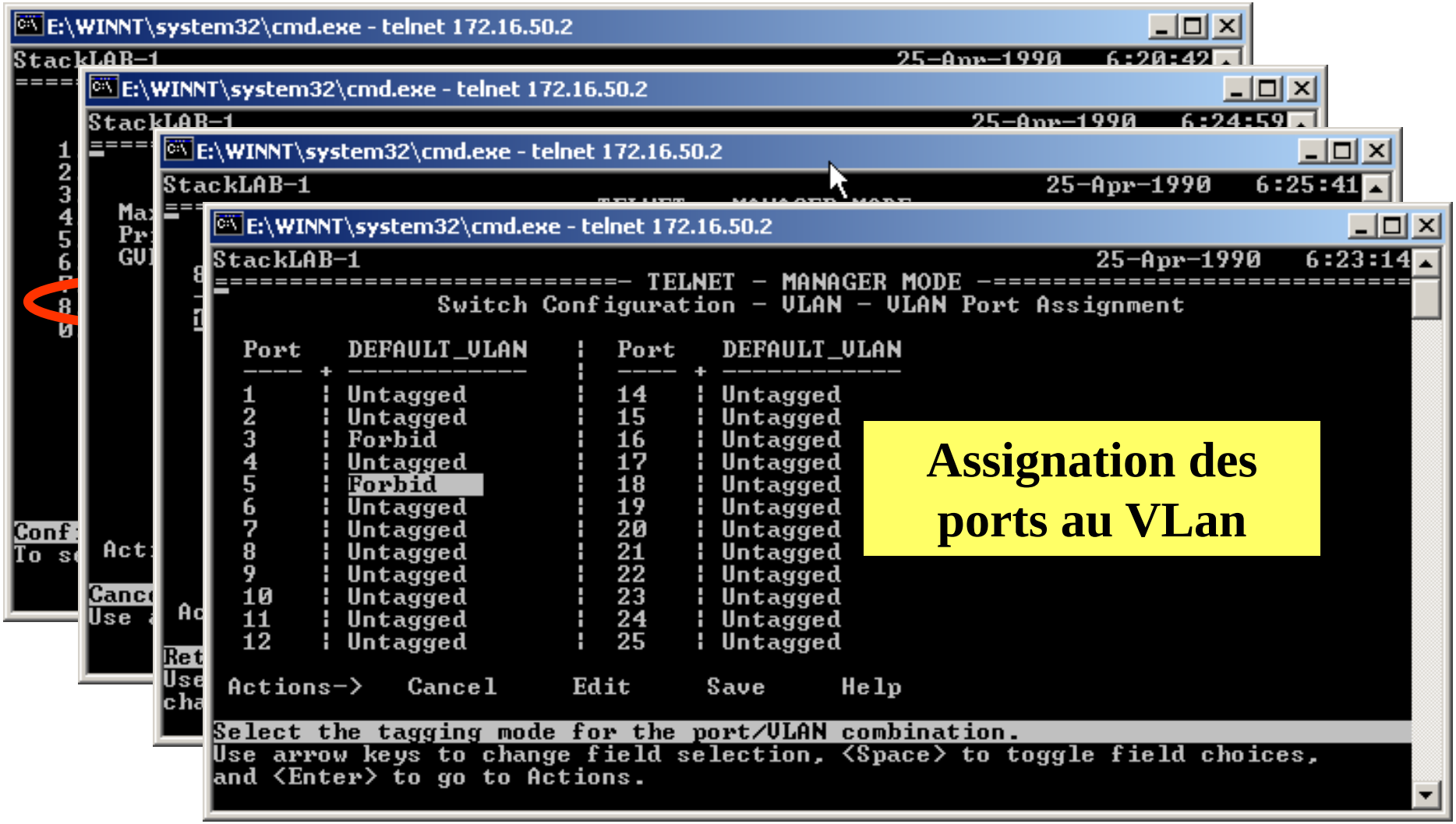

HP Virtual Stack - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris Média
Adresse http://172.16.50.1/
OK Liens
Stack Access: HP - Commander
Stack Closeup
Stack Management
HP ProCurve Switch 2524 - Status: Non-Critical
HP J4813A ProCurve Switch 2524
Identity Status Configuration Security Diagnostics Support
Device View
Fault Detection
System Info
IP Configuration
Port Configuration
Monitor Port
Device Features
Stacking
VLAN Configuration
Support/Mgmt URL
Click on a port or its LED to select it. If you wish to select several ports at once, hold down the Ctrl key while clicking on the additional ports. Click here for the meaning of the port icons.
hp procurve switch 2524 j4813a
Power
Fault
XCVR 25
XCVR 26
For advanced configuration start a telnet session to the switch console.
Select All Ports
Deselect All Ports
Enable Selected Ports
Disable Selected Ports
Fibre op
Switch Number: 0
Switch Number: 1
HP ProCurve Switch 2524
Applet démarrée
Terminé
Internet

Le VLAN



Utilisation de Telnet

Le VLAN


E:\WINNT\system32\cmd.exe - telnet 172.16.50.2
StackLAB-1
25-Apr-1990 6:25:41
E:\WINNT\system32\cmd.exe - telnet 172.16.50.2
StackLAB-1
25-Apr-1990 6:24:59
E:\WINNT\system32\cmd.exe - telnet 172.16.50.2
StackLAB-1
25-Apr-1990 6:23:14
TELNET - MANAGER MODE
Switch Configuration - VLAN - VLAN Port Assignment
Port DEFAULT_VLAN Port DEFAULT_VLAN
1 Untagged 14 Untagged
2 Untagged 15 Untagged
3 Forbid 16 Untagged
4 Untagged 17 Untagged
5 Forbid 18 Untagged
6 Untagged 19 Untagged
7 Untagged 20 Untagged
8 Untagged 21 Untagged
9 Untagged 22 Untagged
10 Untagged 23 Untagged
11 Untagged 24 Untagged
12 Untagged 25 Untagged
Actions-> Cancel Edit Save Help
Select the tagging mode for the port/VLAN combination.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
Assignation des ports au VLan

Le VLAN

- Intérêts du VLAN
  - Le trafic est contrôlé.
  - Le déplacement d'une machine d'un VLAN à un autre se fait simplement par la configuration du switch. Alors qu'un séparation physique des LAN oblige à modifier le câblage (jarretières).
- Inconvénients
  - Augmentation du travail d'administration.
  - Matériels plus coûteux, doivent coopérés entre eux. Les protocoles sont souvent propriétaires.
  - Problème avec les requêtes ARP (broadcast) qui ne peuvent être satisfaites.

Le VPN

Le Virtual Private Network (VPN) trouve son origine dans la recherche d'une interconnexion sécurisée des réseaux locaux au travers des réseaux publics, en particulier de l'Internet (*où l'information circule en clair*).

A l'heure actuelle les VPN se placent surtout dans le contexte de l'Internet.

Note : La technique traditionnelle pour construire un réseau privé est d'utiliser des lignes spécialisée (louée), Numeris ou le RTC (cf. cours sur les réseaux de transports)

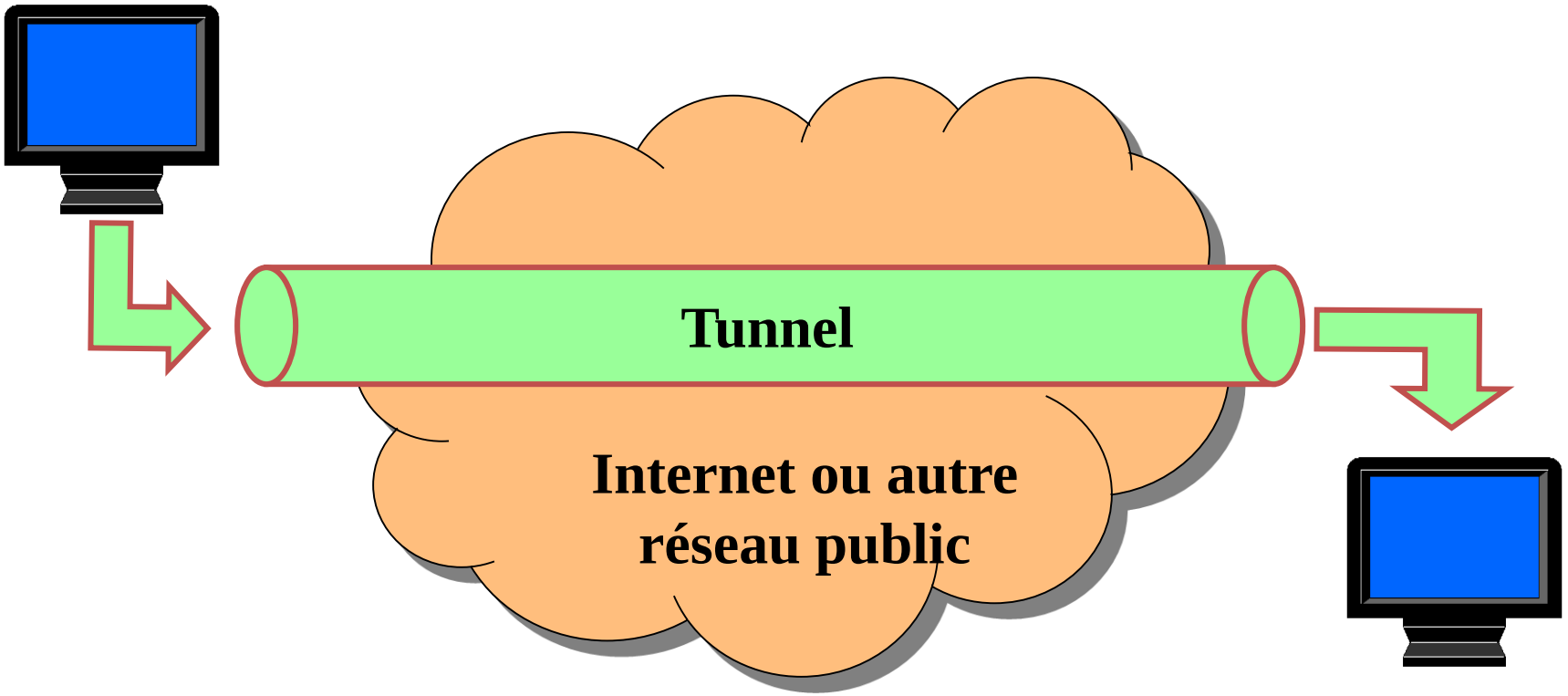
Le VPN

Qu'est-ce qu'un VPN ?

Un réseau privé virtuel permet un échange de données sécurisé et confidentiel entre deux ordinateurs au travers d'un réseau public. Grâce à un principe de tunnel (tunnelling) qui après avoir identifié les deux extrémités fait transiter les données après les avoir cryptées et compressées.

Le VPN

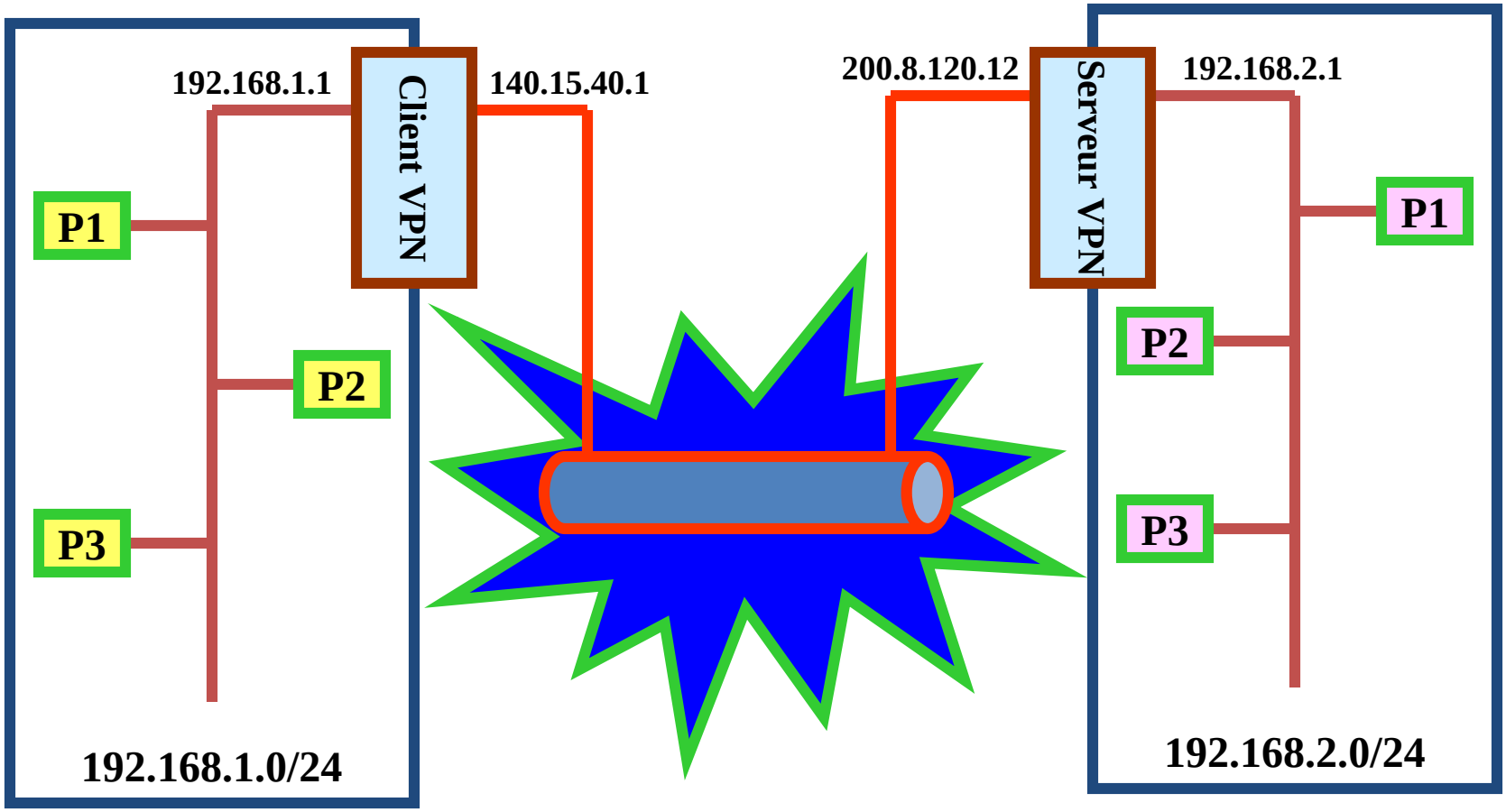
Qu'est-ce qu'un VPN ?



Le tunnel permet d'émuler une connexion point à point au travers d'un réseau public.

Le VPN

Qu'est-ce qu'un VPN ?



Le VPN

Les composants d'un VPN

- Le client VPN initie une connexion vers un serveur VPN. Ce client peut être :
  - ✓ Une station (par exemple un poste mobile qui de l'extérieur crée un VPN avec son entreprise)
  - ✓ Un routeur qui initie un VPN avec un autre routeur. Dans ce cas toutes les stations du réseau local utiliseront le tunnel.

Le VPN

Les composants d'un VPN

- Serveur VPN qui accepte les demandes des clients VPN. Symétriquement le serveur peut donc fournir un :
  - ✓VPN Accès distant (pour un poste "isolé")
  - ✓VPN routeur à routeur

Le VPN

Les composants d'un VPN

- Le tunnel est la portion de connexion dans laquelle les données sont encapsulées. Les tunnels VPN peuvent être établis selon 2 modes :
  - ✓ Le mode volontaire qui correspond à un tunnel entre un client et un serveur VPN.

Le VPN

Les composants d'un VPN

✓ Le mode obligatoire qui est établi par :

- un fournisseur d'accès qui intercepte la demande du client et fait passer ses données dans le tunnel établi.
- L'entreprise entre 2 LAN (routeur à routeur)

Dans ces situations le client ne peut pas éviter le tunnel et n'est pas obliger de posséder le "client VPN".

Le VPN

Les quatre principaux protocoles de VPN sont :

- Au niveau de la couche 2 (liaison)
  - ✓ PPTP : Point to Point Tunnelling Protocole (consortium : Microsoft, 3Com, etc..)
  - ✓ L2F : Layer Two Forwarding (Cisco) (*protocole obsolète)*
  - ✓ L2TP : Layer Two Tunnelling Protocol (de l'IETF – Internet Ingineering Task Force)

Le VPN

Les quatre principaux protocoles de VPN sont :

- Au niveau de la couche 3 (réseau)
  - ✓IPSec : IP Sécurity (de IETF) provient de la nouvelle norme IPv6. IPSec est basé essentiellement sur 4 modules :
    - Internet Key Exchange (IKE) qui prend en charge la gestion et l'échange des clés utilisées pour le cryptage
    - IPComp qui compresse le paquet avant sont chiffrement

Le VPN

- Au niveau de la couche 3 (réseau)
  - ✓IPSec : IP Sécurity (de IETF) provient de la nouvelle norme IPv6. IPSec est basé essentiellement sur 4 modules :
    - Encapsulation Security Payload (ESP) qui chiffrent les paquets
    - Hauthentification Header (AH) qui permet d'authentifier les paquets échangés

Le VPN

Au niveau de la couche 3 (réseau)

- ✓ IPSec est utilisable sous IPv4 et est utilisable aujourd'hui avec tous les systèmes réseau. Il pose néanmoins quelques problèmes :
  - Difficulté de la mise en œuvre.
  - Incompatibilité avec la fonction NAT.
  - Difficulté voire impossibilité de passer au travers des firewall.

Le VPN

Principe

Les protocoles de tunnelling :

- ✓Authentifient les extrémités qui établissent le tunnel.
- ✓Échangent des clés de cryptage.
- ✓Englobent les données ainsi que l'enveloppe de protocole générée par une pile de protocoles puis les chiffrent les compressent et les traitent comme des données pour un autre protocole.

Le VPN

Principe

Le VPN

Les applications traditionnelles des VPN sont :

- L'accès à l'Intranet d'une entreprise depuis l'extérieur (commerciaux en déplacement
- La sécurisation des échanges dans les relations commerciales clients/fournisseurs.

Note : Un VPN peut également être utilisé au sein d'une entreprise sur son réseau local.

Les techniques du filtrage

Le filtrage consiste à intercepter et interpréter les trames au niveau d'une couche (TCP, IP, application,…) et à leur appliquer des règles pour les stopper ou les laisser passer. Le filtrage intervient sur les informations du protocole de la couche et jamais sur les données elles-mêmes. Ainsi, il sera possible d'interdire tous les téléchargements par FTP (ports 20 et 21), mais s'ils sont autorisés le filtre n'arrêtera pas un virus.

Les techniques du filtrage

On peut noter les techniques suivantes dans le filtrage :

- Tout est interdit sauf….
- Tout est autorisé sauf…
- Utilisation d'une liste noire (ce qui est dans la liste est interdit)
- Utilisation d'une liste blanche (ce qui est dans la liste est autorisé)

Les techniques du filtrage

Le filtrage est assuré essentiellement par :

- ✓Le routeur filtrant
- ✓Le Pare Feu ou Firewall
- ✓Le Serveur NAT (Network Adress Translation)
- ✓Le Serveur Proxy

Ces fonctions sont assurées :

- ✓Soit par une machine dédiée avec un système d'exploitation de type Linux ou Windows 200x Server.

Les techniques du filtrage

- ✓Soit par un appareil spécifique
  qui intègre souvent plusieurs fonctions
  Exemple chez le constructeur Cisco

Les routeurs à services intégrés (ISR) Cisco sont fournis avec le cryptage et l'accélération matériels VPN, la version 2.0 de Router & Security Device Manager (SDM) pour une gestion simplifiée et intuitive et un pare-feu VPN basé sur Cisco IOS

(Extrait de la documentation Cisco)

Les techniques du filtrage

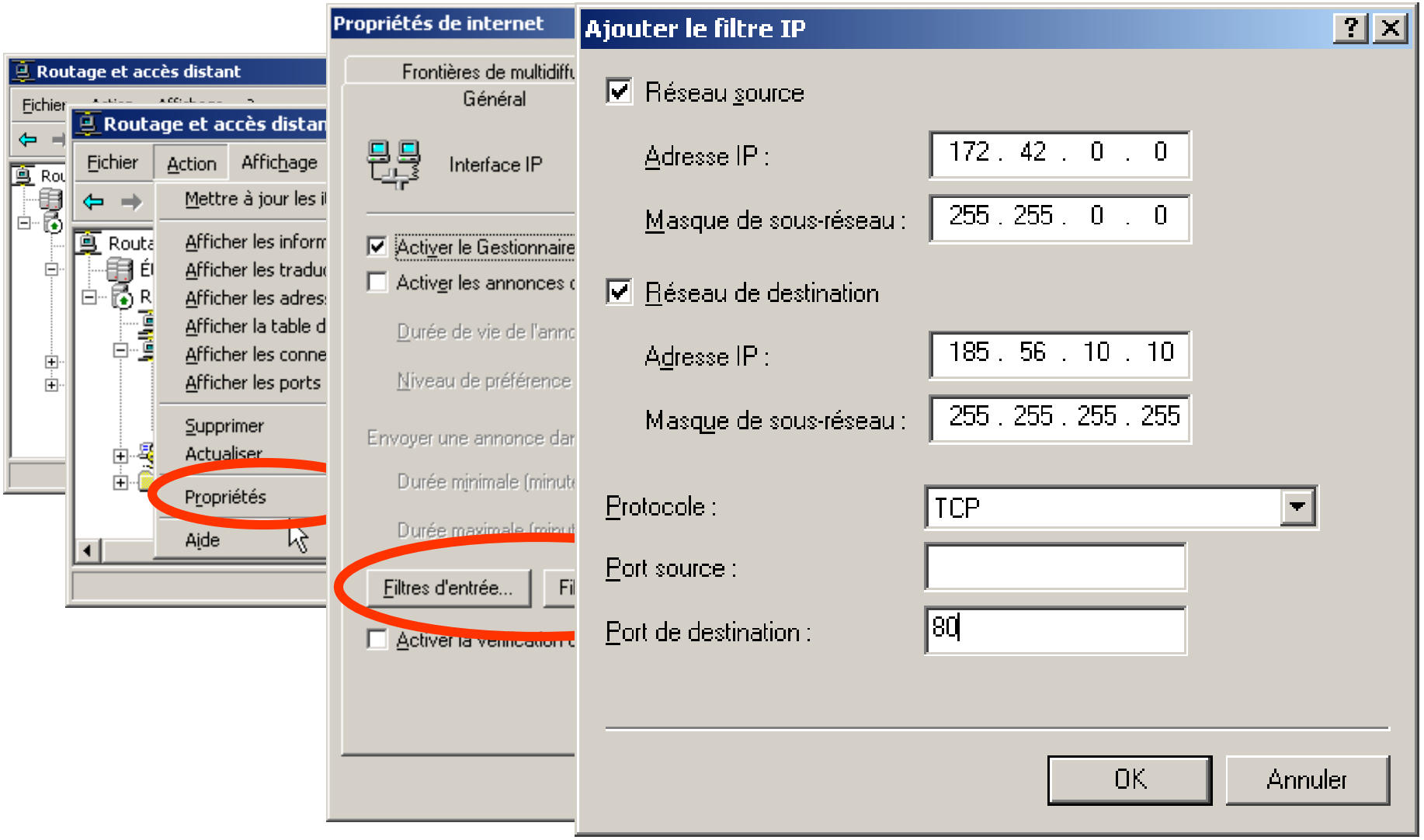
Le ROUTEUR FILTRANT

Un routeur ne filtre pas il aiguille les trames reçues sur une interface vers une autre ; il est transparent.

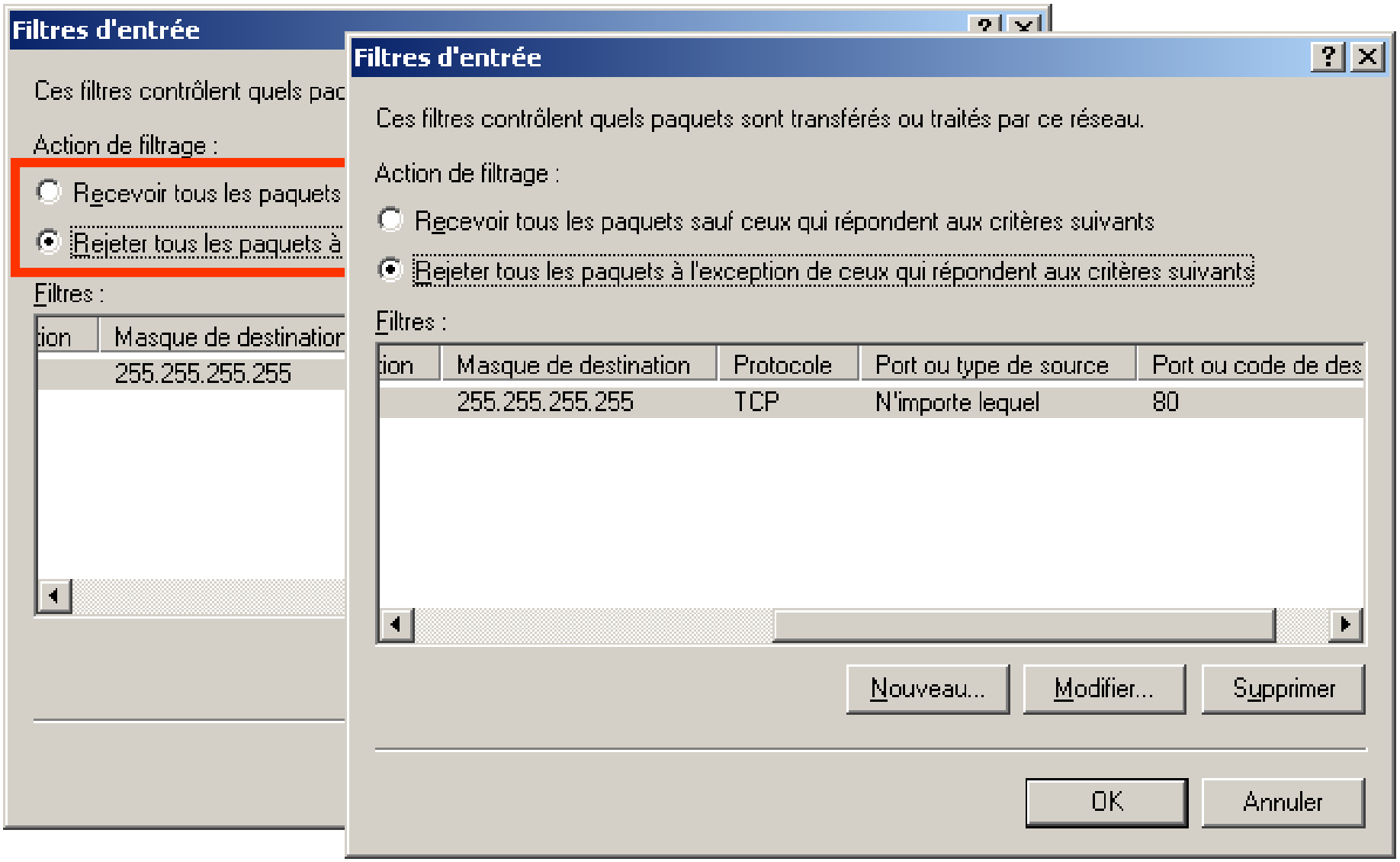
Il est possible de lui ajouter une fonction de filtrage. Ce filtre n'intervient qu'au niveau des transport (TCP) et réseau (IP). Il filtrera donc sur les adresse IP et/ou les ports des trame qui arrive sur chacune de ses interfaces

Les techniques du filtrage

Routeur filtrant sous Windows 2003 Server



Les techniques du filtrage



Les techniques du filtrage

Le PARE-FEU (ou FIREWALL)

Il se caractérise par :

- ✓ Sa portabilité
  Il contrôle le trafic en analysant les données contenues dans les couches 3,4 et 7.
- ✓ Sa situation
  Le pare-feu est un dispositif qui protège l'entreprise des intrusions extérieures. Il doit donc y avoir autant de pare-feu que de "portes" sur l'extérieur, c'est un élément frontal.

Les techniques du filtrage

Le passage par le pare-feu pour entrer dans l'entreprise (dans une moindre mesure pour en sortir) doit être obligatoire. Ceci est imposé par l'architecture du réseau (câblage) et non par une configuration du poste client.

Le pare-feu a obligatoirement plusieurs interfaces réseau

Les techniques du filtrage

Le filtrage peut porter sur :

- ✓les adresses IP,
- ✓les protocoles (TCP, UDP, Telnet, etc.),
- ✓les numéros de port
- ✓Les applications (*passerelle applicative*). Dans ce cas le pare-feu s'intéresse à la nature des données échangée. Un anti-virus et un IDS (Intrusion Detection System) peuvent-être placés à ce niveau.

Note : Un pare-feu est évidemment envisageable entre deux réseaux locaux d'une même entreprise.

Les techniques du filtrage

Certaines applications fixent des numéros de port de façon dynamique et aléatoire (FTP par exemple). Certains firewalls sont capables de s'adapter à ce type de configuration : On parlera d'un filtrage dynamique.

Les techniques du filtrage

Le Serveur NAT (Network Adress Translation)

Devant le manque d'adresses IP disponibles beaucoup d'entreprises disposent de quelques voire une adresse publique et utilisent des adresses IP privées pour leur réseau local (cf. cours TCP/IP).

Ces adresses :

- Ne sont pas routables sur Internet
- Évitent les intrusions sur le réseau local

Les techniques du filtrage

Le serveur NAT va permettre de "translater" les adresses privées en adresses publiques pour que les utilisateurs puissent se connecter sur Internet.

Le serveur NAT de base

Avec NAT il y a une affectation statique à raison d'une d'adresse privée pour une adresse publique. Il y a donc autant d'adresses publiques que privées.

Les techniques du filtrage

Le serveur NAT dynamique

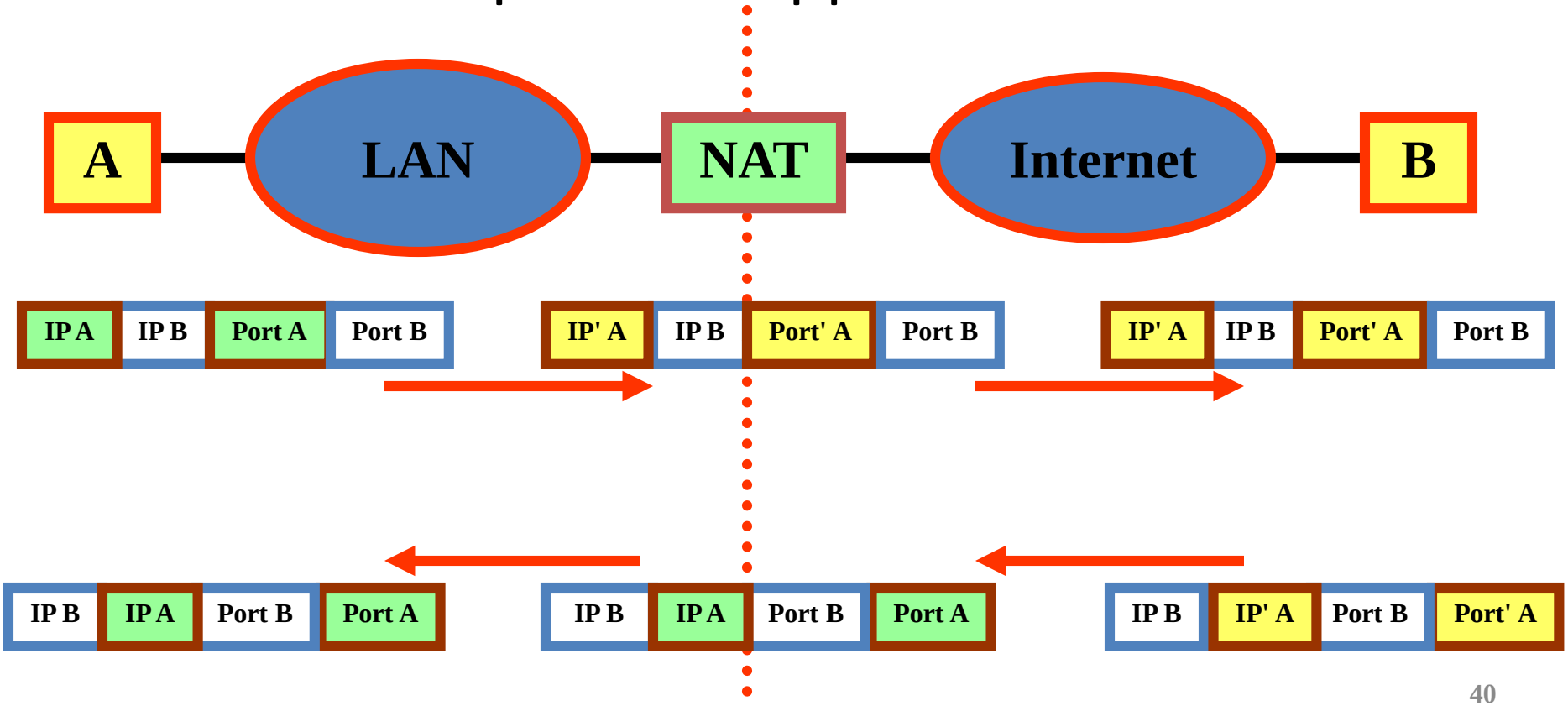
L'adresse publique est affectée dynamiquement à une adresse privée au moment de la connexion. Il n'y a pas d'affectation statique.

Si le nombre d'adresses privées est inférieur au nombre d'adresses publiques (ce qui est très souvent le cas) aucune machine ne pourra accéder à Internet lorsque tous les adresses publiques auront été distribuées.

Les techniques du filtrage

Le serveur NAPT (Network Adress and Port Translation)

Cette méthode consiste à translater l'adresse IP et le numéro du port de l'application visée.



Les techniques du filtrage

Le serveur PROXY

Le serveur PROXY se situe au niveau des protocoles applicatifs (HTTP, FTP, etc.) ; on parlera ainsi d'un Proxy Web ou proxy HTTP.

Le serveur Proxy est un serveur mandataire ; En d'autres termes l'application (navigateur par exemple) va lui transmettre sa demande qu'il redirigera après contrôle vers son destinataire.

Il peut y avoir plusieurs proxy

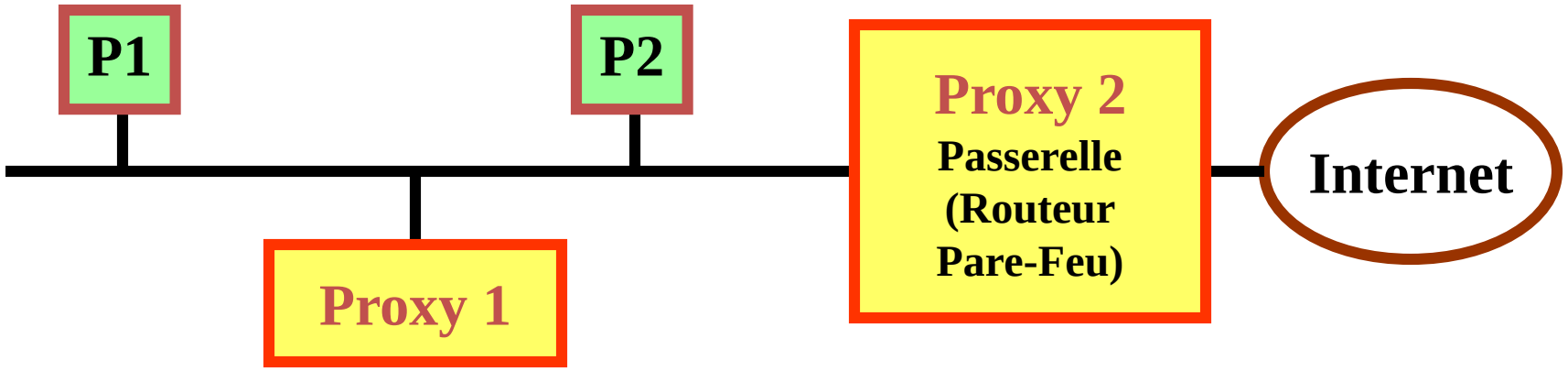
Les techniques du filtrage

Les principales fonctions d'un Proxy :

- ✓ Mise en Cache. Le proxy sauvegarde les pages visitées afin de les redonner plus rapidement.
- ✓ Le filtrage. Le filtre concerne les requêtes de l'application (URL, Port par exemple). Le filtrage peut porter sur le contenu (mots-clés en général) reçu par le proxy avant de le retransmettre au client.
- ✓ L'authentification du client

Les techniques du filtrage

La situation du serveur Proxy sur le réseau n'est pas indifférente



L'utilisateur peut passer outre le Proxy 1 en modifiant la configuration de l'application cliente. Par contre le passage par le Proxy 2 est rendu obligatoire de par sa situation.

Les techniques du filtrage

Conclusion

Chaque technique présentée assure une fonction particulière et est supportée ici par un serveur.

On se rend compte également que certaines fonctions se retrouvent plusieurs fois (filtrage adresses IP et ports dans le pare-feu et le routeur filtrant par exemple).

Matériellement ces serveurs se retrouvent dans des propositions commerciales qui "mélangent" ces fonctions.

Zone "démilitarisée" (DMZ)

La DMZ permet de sortir du réseau local les serveurs ayant un accès public. La DMZ est une zone tampon entre l'Internet et le réseau local.

Ces serveurs possèdent en général des adresses IP publiques (elles peuvent être aussi privées) alors que le réseau local possède des adresses privées.

Ainsi la DMZ est accessible depuis l'Internet et le réseau local. Par contre les trames provenant de l'Internet ne circulent pas sur le réseau local.

Zone "démilitarisée" (DMZ)