**PRODUCTION ASSOCIEE**

**Contexte :**

Le contexte de la Maison des Ligues de Lorraine (La M2L) a été retenu au sein de notre centre de formation dans le cadre des PPE. La M2L, établissement du Conseil Régionalde Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d’autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l’ensemble des ligues sportives installées. Elle assure l’offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région.

L’une des préoccupations de l’administrateur est d’automatiser au maximum des tâches administratives pour répondre rapidement aux différentes sollicitations des départements de la M2L et des ligues sportives. C’est dans ce contexte que j’ai participé, avec d’autres élèves de mon groupe, au projet consistant à créer des VLANs, configurer les routeurs en OSPF et à mettre en place un serveur TSE pour permettre aux utilisateurs d’une ligue sportive de travailler à distance sur une application commune, la suite bureautique Open Office ou d’autres applications dans notre cas.

**RESEAU :**

Le réseau de la M2L est organisé VLANs et comporte des commutateurs de niveau 2 et des routeurs.

Le VLAN INFORMATIQUE est dédié aux serveurs : contrôleur de domaine, DHCP et serveur d’applications. Les ligues sont organisées aussi en VLANs. Au niveau du domaine la M2L et les ligues sont représentées en unités d’organisation. Les serveurs sont en Windows 2003 SP2 & les clients en Windows XP SP3 ou Seven.

**Liste du matériel :**

3 routeurs Cisco

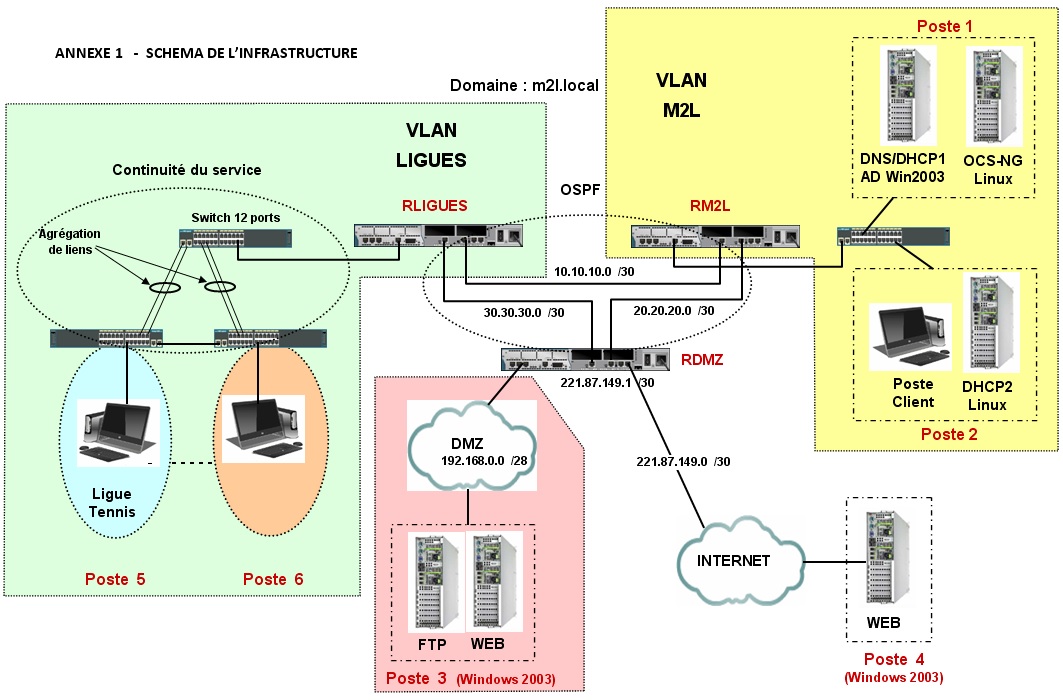
4 switch cisco

2 switch non manageable

Serveur 2003 vistualisé

Postes clients XP

**Schéma :**

****

Pour les liaisons entre routeurs/routeurs et les switchs/switchs, on utilise des câbles croisé. Pour les liaisons entre switch et routeurs on utilise des câbles droits.

Les routeurs utilisent le protocole OSPF (Open Shortest Path First), c’est un algorithme dynamique  à état de liens, qui permet de mettre à jour la table de routage automatiquement grâce aux messages hello échangés entre les routeurs.

Les switchs sont reliés aux routeurs par un lien Trunk, c’est un lien qui permet de faire transiter plusieurs VLANs sur un seul lien physique.

Afin d’éviter une situation de tempête de diffusion, on utilise le protocole spanning-tree qui permet de mettre fin à une tempête de broadcast en coupant temporairement un lien afin de cassé la boucle.

**CONFIGURATION :**

**----------------------------------**CONFIG RESEAU----------------------------------------------

Mot de passe console : cisco

Administration à distance (SSH) : login : admin MDP : admin

##### Adresses de gestion :

RouterM2L : 10.10.10.2

RouterLIGUES : 10.10.10.1

RouterDMZ : 20.20.20.2

SWLIGUE1 : 172.16.99.17

SWLIGUE2 : 172.16.99.18

SWLIGUE3 : 172.16.99.19

SWM2L : 172.16.99.1

SWDMZ : 172.16.99.33

--------------------------------RouterM2L---------------------------------

en

conf t

hostname RouterM2L

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int fa 0/1

ip address 10.10.10.2 255.255.255.252

no shutdown

exit

int fa 0/0

ip address 20.20.20.1 255.255.255.252

no shutdown

exit

int eth 1/0

no shutdown

exit

int eth 1/0.2

encapsulation dot1Q 2

ip address 172.16.0.62 255.255.255.192

exit

int eth 1/0.3

encapsulation dot1Q 3

ip address 172.16.0.126 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Eth 1/0.99

encapsulation dot1Q 99

ip address 172.16.99.14 255.255.255.240

exit

router ospf 1

network 172.16.0.0 0.0.0.63 area 0

network 172.16.0.64 0.0.0.63 area 0

network 172.16.99.0 0.0.0.15 area 0

network 10.10.10.0 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

passive-interface Ethernet 1/0

exit

--------------------------------RouterLIGUES-------------------------------------

en

conf t

hostname RLIGUES

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int Fa 0/1

ip address 10.10.10.1 255.255.255.252

no shutdown

exit

int Eth 1/0

ip address 30.30.30.2 255.255.255.252

no shutdown

exit

int Fa 0/0

no shutdown

exit

int Fa 0/0.10

encapsulation dot1Q 10

ip address 172.16.10.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.11

encapsulation dot1Q 11

ip address 172.16.11.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.12

encapsulation dot1Q 12

ip address 172.16.12.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.99

encapsulation dot1Q 99

ip address 172.16.99.30 255.255.255.240

exit

router ospf 1

network 172.16.10.0 0.0.0.63 area 0

network 172.16.11.0 0.0.0.63 area 0

network 172.16.12.0 0.0.0.63 area 0

network 172.16.99.16 0.0.0.15 area 0

network 10.10.10.0 0.0.0.3 area 0

network 30.30.30.0 0.0.0.3 area 0

passive-interface FastEthernet 0/0

end

--------------------------------------RouterDMZ--------------------------------

en

conf t

hostname RDMZ

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int fa 0/0

ip address 20.20.20.2 255.255.255.252

ip nat inside

no shutdown

exit

int fa 0/1

ip address 221.87.149.6 255.255.255.248

ip nat outside

ip access-group 100 in

no shutdown

exit

int Eth 1/0

ip address 30.30.30.1 255.255.255.252

ip nat inside

no shutdown

exit

int Eth 1/1

ip address 192.168.0.14 255.255.255.240

ip nat inside

ip access-group 102 in

no shutdown

exit

router ospf 1

network 30.30.30.0 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

network 192.168.0.0 0.0.0.15 area 0

passive-interface Ethernet 1/1

default-information originate

exit

ip route 0.0.0.0 0.0.0.0 fa0/1

access-list 10 permit 172.16.0.0 0.0.255.255

ip nat inside source list 10 interface fa0/1 overload

ip nat inside source static tcp 192.168.0.5 80 221.87.149.6 80

ip nat inside source static tcp 192.168.0.5 443 221.87.149.6 443

! ----------- Filtrage Firewall -------------------

access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established

access-list 100 permit tcp any host 192.168.0.13 eq 80

access-list 100 permit tcp any host 192.168.0.13 eq 443

access-list 100 permit tcp any host 192.168.0.12 eq 21

access-list 100 permit tcp any host 192.168.0.12 eq 20

access-list 100 permit icmp any host 172.16.0.54 echo-reply

access-list 100 permit icmp any host 172.16.0.55 echo-reply

access-list 100 permit icmp any host 172.16.0.54 unreachable

access-list 100 permit icmp any host 172.16.0.55 unreachable

access-list 102 permit icmp any host 172.16.0.54 echo-reply

access-list 102 permit icmp any host 172.16.0.55 echo-reply

access-list 102 permit icmp any host 172.16.0.54 unreachable

access-list 102 permit icmp any host 172.16.0.55 unreachable

-----------------------------------------SWLIGUE1-----------------------------------------------------

en

conf t

hostname SW1LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/2-3

channel-group 1 mode on

exit

int port-channel1

switchport mode trunk

switchport nonegotiate

exit

int range fa 0/4-5

channel-group 2 mode on

exit

int port-channel2

switchport mode trunk

switchport nonegotiate

exit

int fa 0/1

switchport mode trunk

exit

VLAN 99

name GESTION

exit

int VLAN 99

ip address 172.16.99.17 255.255.255.240

ip default-gateway 172.16.99.30

exit

-------------------------------------SWLIGUE2-----------------------------------

en

conf t

hostname SW2LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/1-2

channel-group 1 mode on

int port-channel1

switchport mode trunk

switchport nonegotiate

VLAN 10

name ATHLE

VLAN 11

name TENNIS

VLAN 12

name BASKET

VLAN 99

name GESTION

int VLAN 99

ip address 172.16.99.18 255.255.255.240

ip default-gateway 172.16.99.30

int range fa 0/4-8

switchport mode access

switchport access VLAN 10

spanning-tree portfast

exit

int range fa 0/8-12

switchport mode access

switchport access VLAN 11

spanning-tree portfast

exit

int fa 0/3

switchport mode trunk

exit

---------------------------------------SWLIGUE3---------------------------------------------

en

conf t

hostname SW3LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/1-2

channel-group 1 mode on

exit

int port-channel1

switchport mode trunk

switchport nonegotiate

exit

VLAN 10

name ATHLE

exit

VLAN 11

name TENNIS

exit

VLAN 12

name BASKET

exit

VLAN 99

name GESTION

exit

int VLAN 99

ip address 172.16.99.19 255.255.255.240

ip default-gateway 172.16.99.30

exit

int range fa 0/4-8

switchport mode access

switchport access VLAN 12

spanning-tree portfast

exit

int fa 0/3

switchport mode trunk

exit

---------------------------------------SWM2L------------------------------------------------------

en

conf t

hostname SWM2L

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

VLAN 2

name INFO

exit

VLAN 3

name ADMIN

exit

VLAN 99

name GESTION

exit

int fa 0/1

switchport mode trunk

switchport nonegotiate

exit

int range fa 0/2-11

switchport mode access

switchport access VLAN 2

spanning-tree portfast

exit

int range fa 0/12-16

switchport mode access

switchport access VLAN 3

spanning-tree portfast

exit

int VLAN 99

ip address 172.16.99.1 255.255.255.240

ip default-gateway 172.16.99.14

exit

**LE SYSTEME :**

Nous utiliserons le logiciel Virtual Box afin de simulée un environnement Windows Serveur 2003, qui joue le rôle de Contrôleur du domaine –Serveur DHCP- Serveur TSE :

-le contrôleur de domaine reflètera l’organisation de la Maison des Ligues, nous y trouverons ainsi les différentes représentées sous forme d’unité d’organisation.

- Serveur DHCP (Dynamic Host Configuration Protocol) : Ce protocole dont le rôle est d’assurer la configuration automatique des paramètres IP d’une [station](http://fr.wikipedia.org/wiki/Station_de_travail), notamment en lui affectant automatiquement une [adresse IP](http://fr.wikipedia.org/wiki/Adresse_IP) et un [masque de sous-réseau](http://fr.wikipedia.org/wiki/Masque_de_sous-r%C3%A9seau). Nous allons créer différents plage d’adresse IP pour les différents Ligues de la M2L.

-Serveur TSE (Terminal Server) : Ce service que propose Microsoft, permet à un utilisateur d'accéder à des applications et des données sur le Serveur hébergeant ce service.

**MISE EN PLACE D’UN SERVEUR D’APPLICATION :**

**Serveur d’application et connexion à distance :**

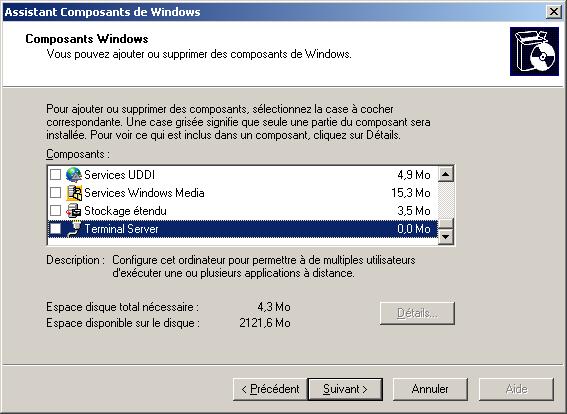
Comme le serveur de fichiers met des fichiers à dispositions d’utilisateurs, le serveur d’applications permet à des utilisateurs connectés en réseau d’accéder à des logiciels applicatifs à partir d’un exemplaire unique situé sur le serveur d’application.

**1°) Installation et Gestion du service Terminal Server**

1. **Sur le serveur**

Se diriger vers le Panneau de Configuration puis Ajout/Suppression de Programmes "Ajout/Suppression de composants Windows ".

Dans la liste des composants, cocher la case correspondant à Terminal Server. (CD d’installation nécessaire)



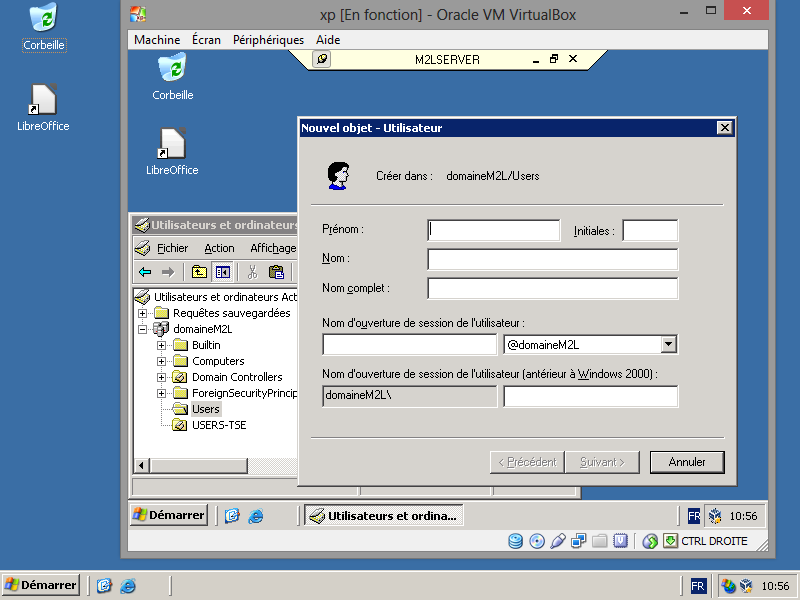
Un redémarrage du serveur est nécessaire après l’installation des services.

*Il faut noter qu'à la différence de Windows 2000, le service Terminal Server de Windows Server 2003 s'installe directement en mode Application. Il n'y a plus le choix d'installer notre serveur en mode Administration à distance pour la simple et bonne raison que ce dernier a été remplacé par le bureau à distance.*

**Configuration**

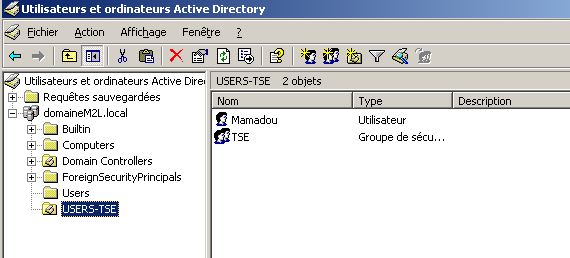
Par défaut, seuls les membres des groupes administrateurs et utilisateurs de bureau à distance peuvent ouvrir une session sur un terminal server.  
Donc on peut accéder au server depuis un poste client afin d’administrer à distance le server.

Pour cela il suffit de lancer l’accès au bureau à distance sur XP, renseigner le nom du server puis se connecter en tant administrateur et voilà on a la main sur le Server.



Pour les autres utilisateurs, on va mesure de sécurité, crée une unité d’organisation dans laquelle on insère un groupe avec des utilisateurs, puis on ajoute une stratégie de groupe pour limiter les droits des utilisateurs, dans les accès au serveur en TSE.

L’unité d’organisation en question sera nommée USERS-TSE dans laquelle on crée un groupe TSE et y mettre un utilisateur Mamadou.



nous appliquerons une stratégie de groupe afin d’appliqué une sécurité pour empecher l’utilisateur d’avoir tous les droits sur le server d’application.

Clique droit sur le groupe « USERS-TSE » aller dans propriété puis stratégie de groupe

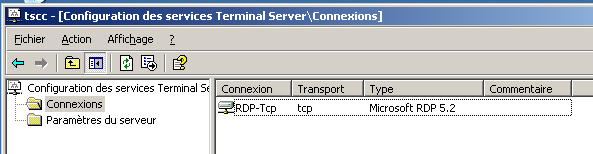
On editera une nouvelle stratégie qui enlevera certains attributs comme l’accès au panneau de configuration .

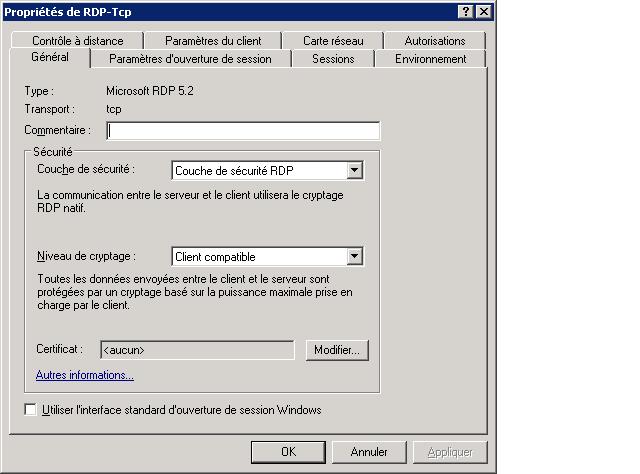
Nous pouvons par ce biais définir la façon dont notre serveur réagira lorsque des connexions clientes seront établies. Nous pouvons aussi personnaliser l'environnement de chaque utilisateur. Et tout ceci de façon centralisée. Pour ce faire, nous ouvrons la console des stratégies locales (GPEDIT.MSC) et nous développons le nœud Configuration ordinateur => Modèles d'administration =>Composants Windows => Services Terminal Server :



**Configuration des services Terminal Server**

La configuration des services de Terminal Server s’effectue à partir d’une console, qui se trouve dans :

Démarrer🡪Outils d’administrations🡪Configuration des services Terminal Server.  
Dans connexions, il suffit de faire un clic droit, puis propriétés sur RDP-TCP pour avoir accès aux propriétés de connexions de TSE.  




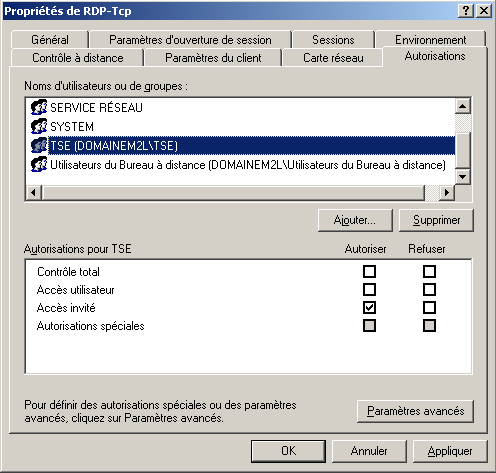
Dans ces onglets :

**- Général**: renseigne le niveau de protection du cryptage.  
**- Sessions**: Définie des règles, temps maximum de connexions.

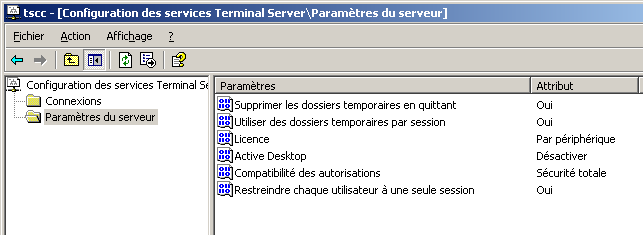
**- Environnement**: Application qui sera ouverte à la connexion de la session Terminal Server si on le désire.

**- Carte réseau**: Interface réseau qu’utilisera Terminal Server, il permet également de limiter le nombre de connexions.  
**- Autorisations**: Permet d’indiquer les groupes ou utilisateurs autorisés à ouvrir une session terminal server.

C’est dans l’onglet Autorisations qu’il va falloir ajouter le groupe TSE, pour que les utilisateurs puissent se connecter et utiliser des applications partagées.

****

Dans paramètres :



- **Supprimer les dossiers temporaires en quittant** : ce paramètre permet de déterminer si l'on souhaite que les dossiers temporaires créés lors de la connexion de soient conservés à la fermeture de la session du client ou non.

- **Utiliser des dossiers temporaires par session** : ce paramètre détermine le fait que chaque utilisateur ouvrant une session utilisera un dossier temporaire différent (plutôt qu'un dossier temporaire commun à tous les utilisateurs).

- **Licence** : ce paramètre définit le type de licences que nous voulons utiliser sur notre serveur Terminal Server. Il en existe deux : les licences par périphériques et les licences par utilisateurs.

- **Active Desktop** : ce paramètre indique si la fonctionnalité Active Desktop doit être activée ou non.

- **Compatibilité des autorisations** : permet de spécifier si nous voulons donner un accès au registre ou à certains répertoires système à certaines applications anciennes. Dans ce cas nous choisirons l'option Sécurité moyenne. Dans d'autres situations où les applications ont été écrites de façon à utiliser les fonctionnalités de Windows Server 2003, nous pouvons conserver l'option Sécurité totale. Dans ce cas, l'accès au registre et à certains dossiers système n'est pas autorisé. Ce paramètre est celui par défaut.

- **Restreindre chaque utilisateur à une seule session** : cette option limite le nombre de sessions ouvertes par chaque utilisateur à une seule. De cette façon, un utilisateur qui aurait simplement déconnecté sa précédente session rouvrira cette dernière. Encore une fois cela permet d'économiser des ressources sur le serveur.

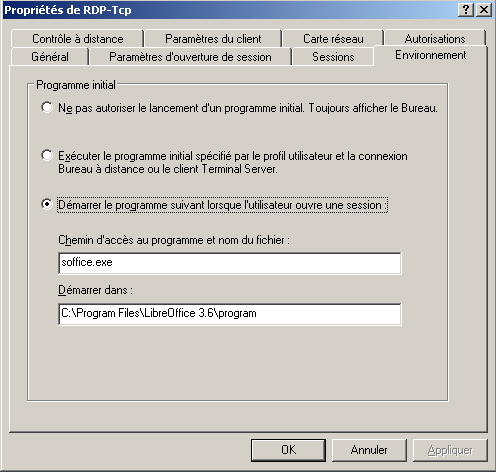
**Installation d'applications**

Utiliser l'option Ajout/Suppression de programme dans le Panneau de configuration. Cela passe automatiquement notre serveur en mode installation et le repasse en mode exécution une fois l'installation achevée. (dans notre exemple on va installer Libroffice)

Après l’installation de l’application, on va paramétrer TSE afin que dès qu’un utilisateur ouvre une session TSE

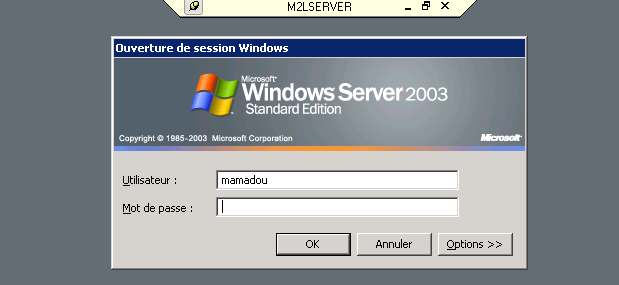
L’application précédemment installer s’exécute ainsi l’utilisateur n’aura accès qu’à l’application ce ceci est une autre façon de renforcer la sécurité.

Pour cela nous allons configurer **l’Environnement** du TSE dans les Propriétés de RDP-Tcp

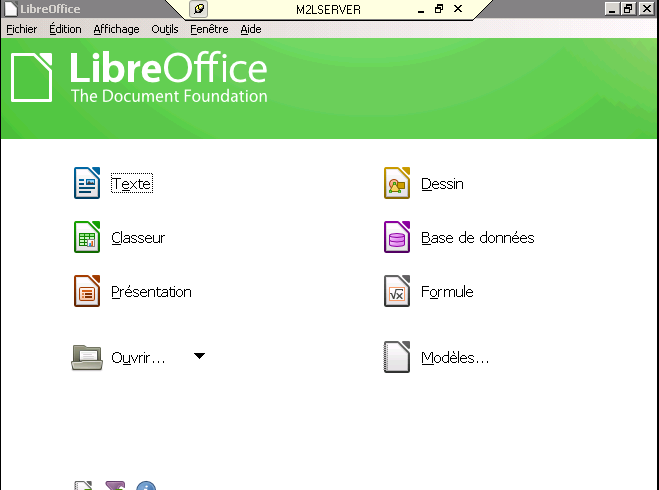


**Sur le poste client**

La connexion s’effectue grâce à la connexion du bureau à distance.  
Aller dans Démarrer🡪Tous les programmes🡪Accessoires🡪Communication🡪Bureau à distance.  
Il suffit alors de renseigner l’adresse IP du serveur avec le nom d’utilisateur avec son mot de passe.



On a accès alors au serveur d’application en mode TSE.



**BATTERIE DE TESTS :**

* Connexion en utilisant une session d’un utilisateur autorisé à se connecter sur le Terminal Server.
* Connexion en utilisant une session d’un utilisateur non autorisé à se connecter sur le Terminal Server.
* Vérifier que l’environnement est bien celle choisit dans la stratégie de groupe.
* Test de non régression pour les autres utilisateurs de Terminal Server.