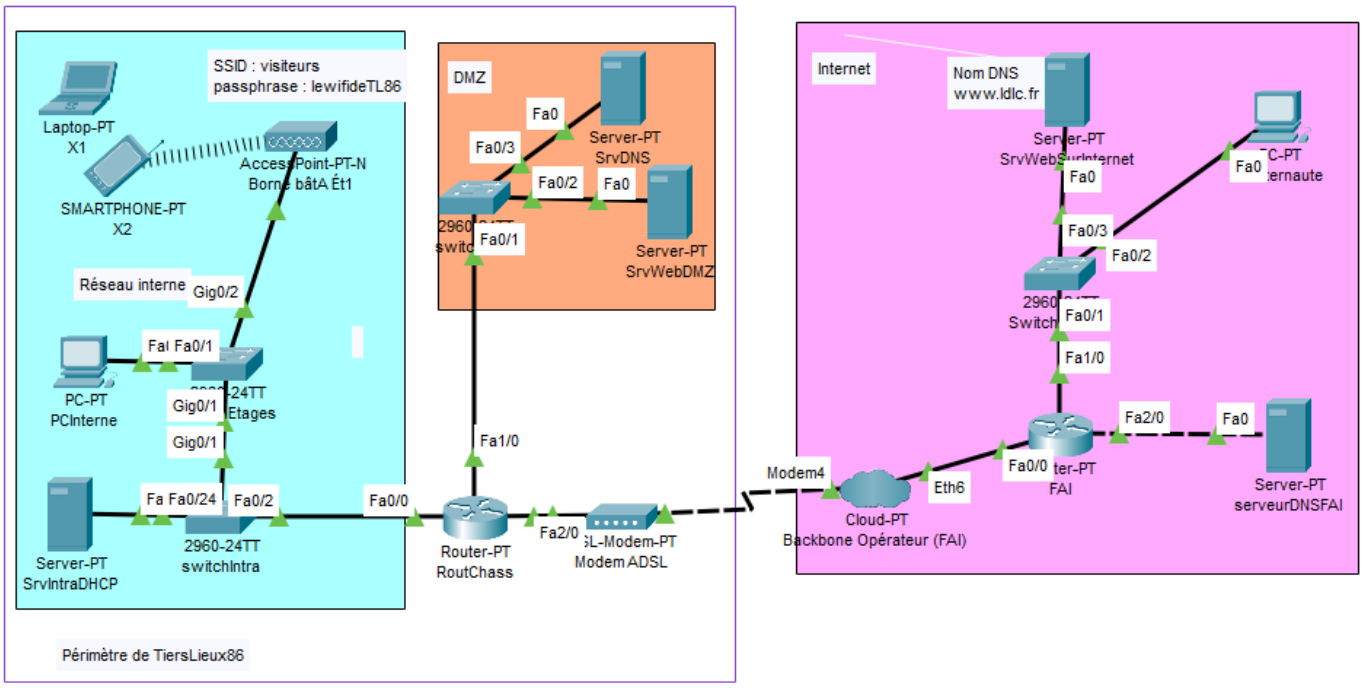
Atelier 3 : EvolInfra

Sommaire

Mission 1 : maquettage et serveur NTP

Tâche 1

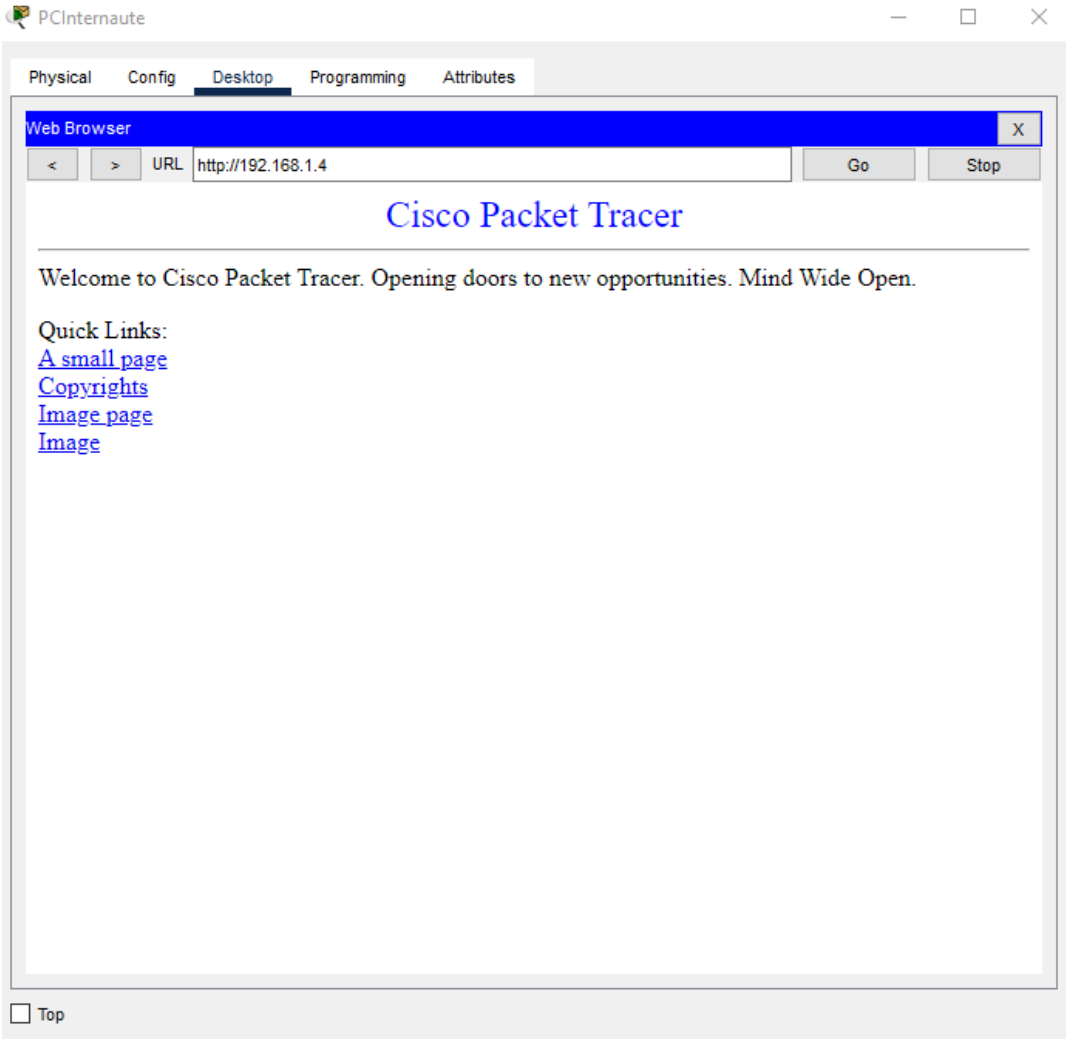


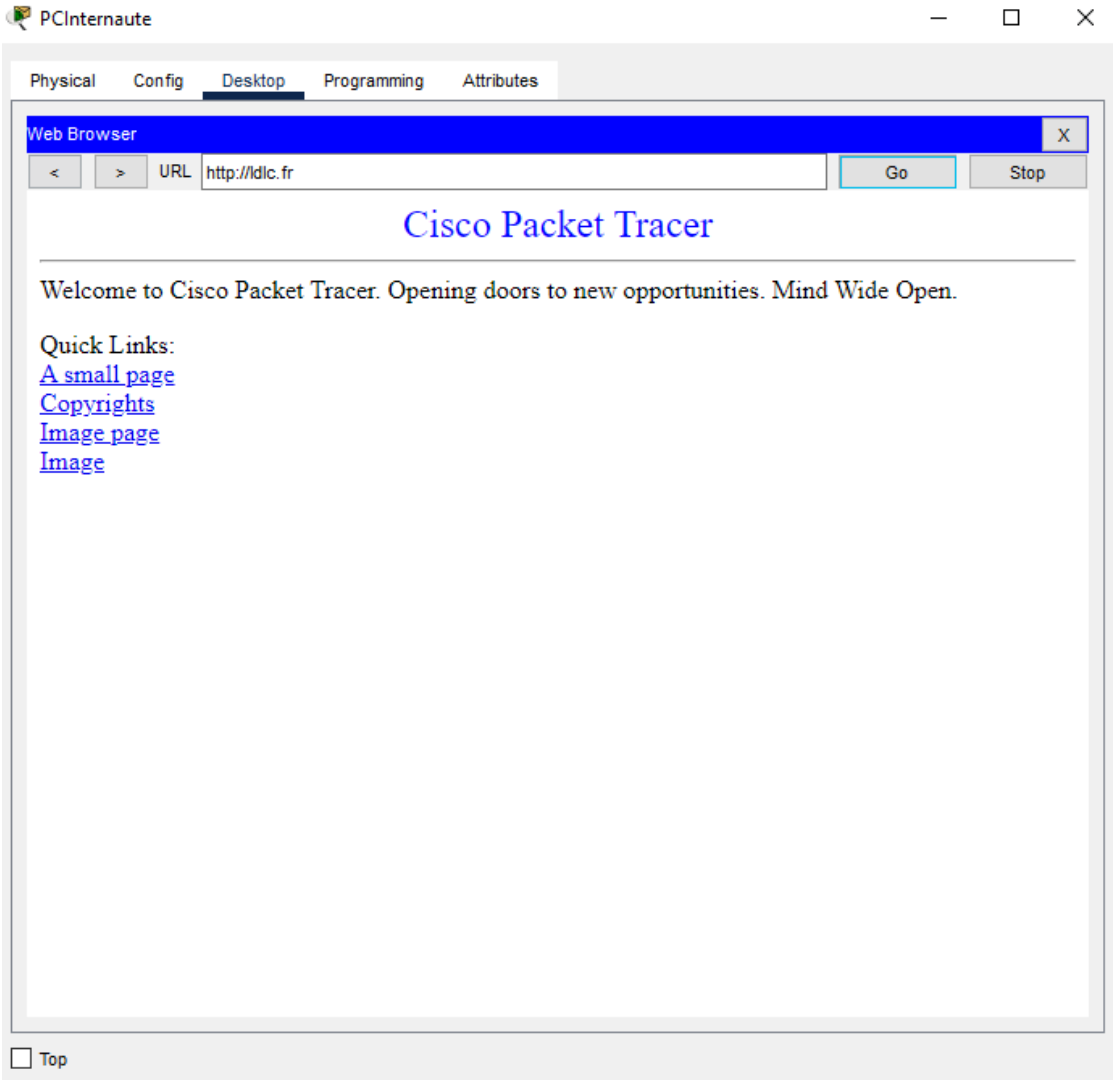
Tâche 2

Configurer la partie internet sous Packet Tracer, comprenant un routeur de FAI et son serveur DNS, un serveur Web sur internet et un pc d'un internaute lambda. Vous configurerez les adresses IP et le serveur DNS pour permettre l'accès au site web externe par son url (ex : www.ldlc.fr pour l'IP 91.211.165.65).

On peut remarquer que le ping vers l'adresse IP fonctionne bien car on arrive à accéder à la page web mais aussi mais en mettant le nom cela fonctionne aussi.

J'ai changé l'adresse IP car je préférer en prendre une plus simple et plus facile à retenir afin de faire la configuration ensuite.


PCInternaute
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.4
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top

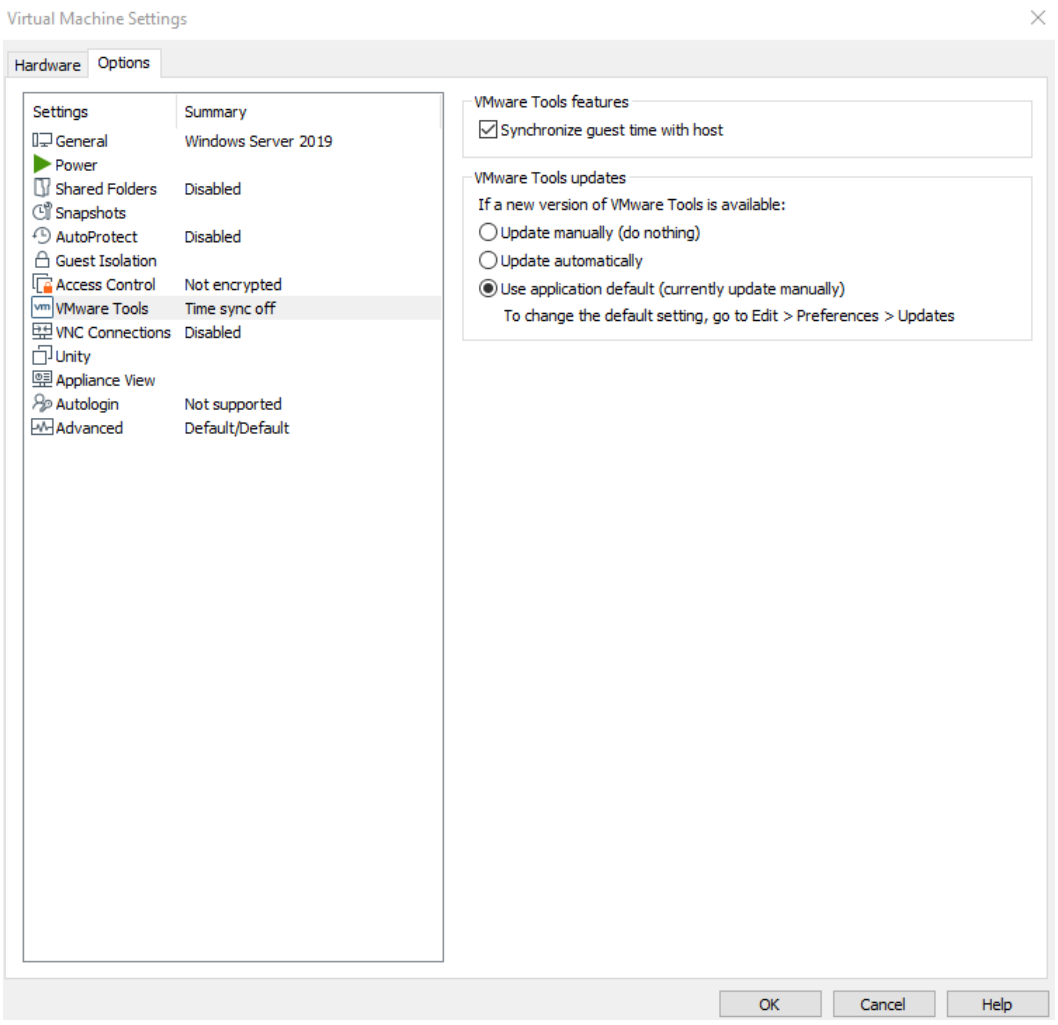



```
Switch(config)#int vlan30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#
```

Tâche 3

Installer et configurer un serveur de temps (Service NTP) sur un serveur Windows (ou Linux), tous les postes de travail, serveurs et équipements réseaux devront être synchronisés à ce serveur.

J’ai activé la synchronisation via mes paramètres de VMWare.



Restart-Service w32time

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> w32tm /config /manualpeerlist:TiersLieux86.fr /syncfromflags:manual
La commande s'est terminée correctement.
PS C:\Users\Administrateur> Restart-Service w32time
PS C:\Users\Administrateur>
```

Éditeur du Registre

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
NtpServer	REG_SZ	TiersLieux86.fr
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
ServiceDllUnloa...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	SvchostEntry_W32Time
Type	REG_SZ	NTP

w32tm /query /status

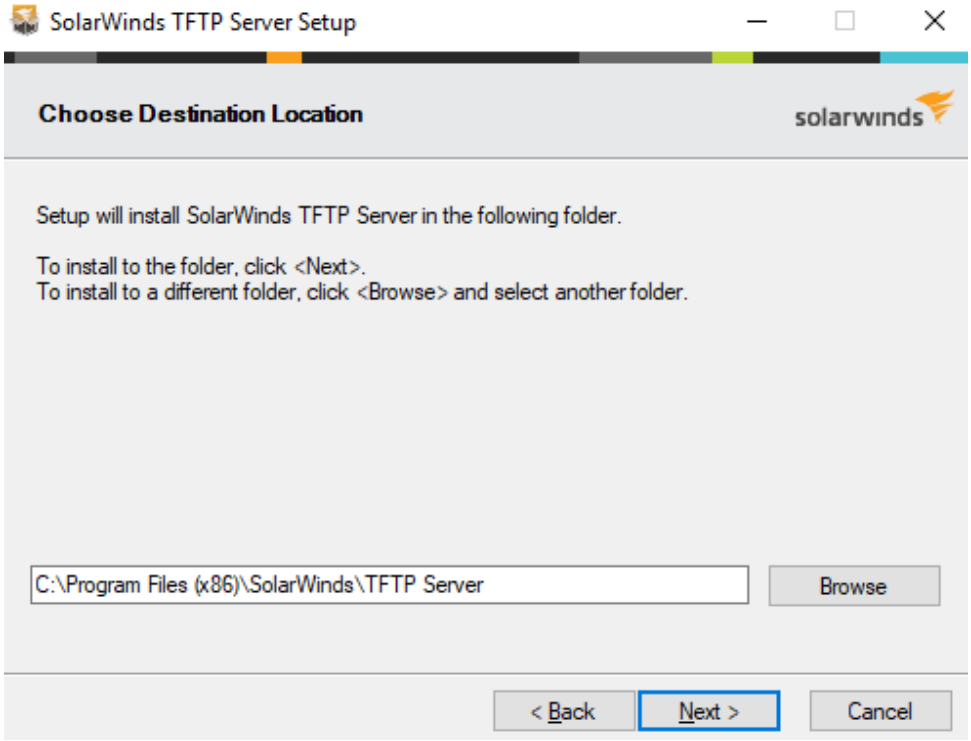
```
PS C:\Users\Administrateur> w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 1 (Référence principale, synchronisée par l'horloge du réveil)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0000000s
Dispersion de racine : 10.0000000s
ID de référence : 0x4C4F434C (Nom de la source :  "LOCL")
Heure de la dernière synchronisation réussie : 30/03/2023 14:54:40
Source : TiersLieux86.fr
Intervalle d'interrogation : 6 (64s)

PS C:\Users\Administrateur>
```

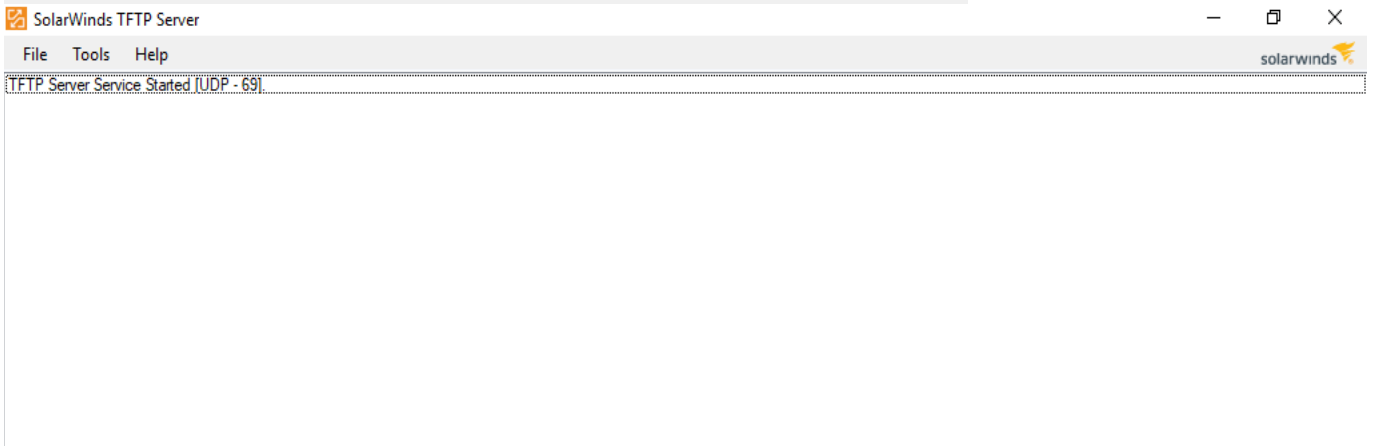
J'ai utilisé la commande suivante pour que le message apparaisse : w32tm /resync

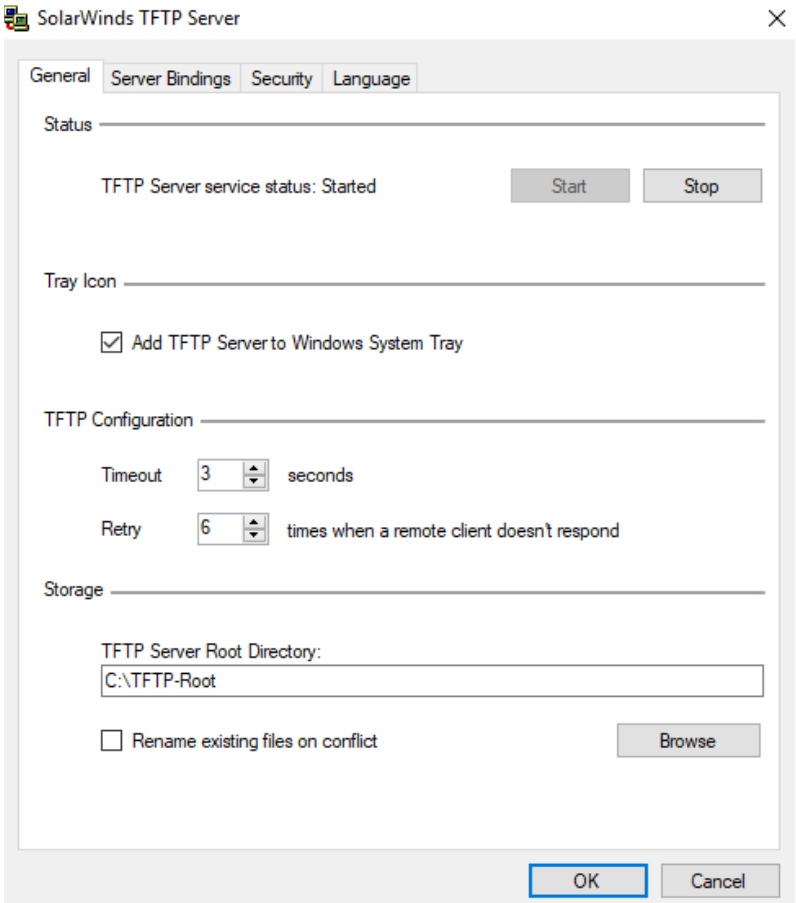
```
Envoi de la commande de resynchronisation à l'ordinateur local
La commande s'est terminée correctement.
```

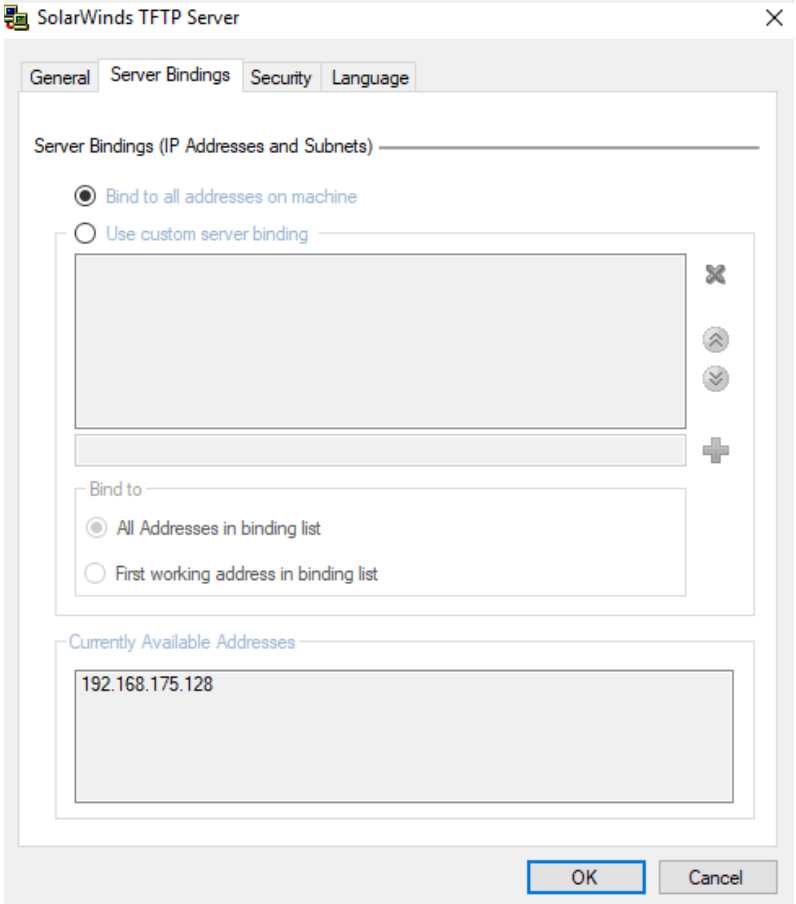
Mission 2 : sauvegarde des équipements réseau

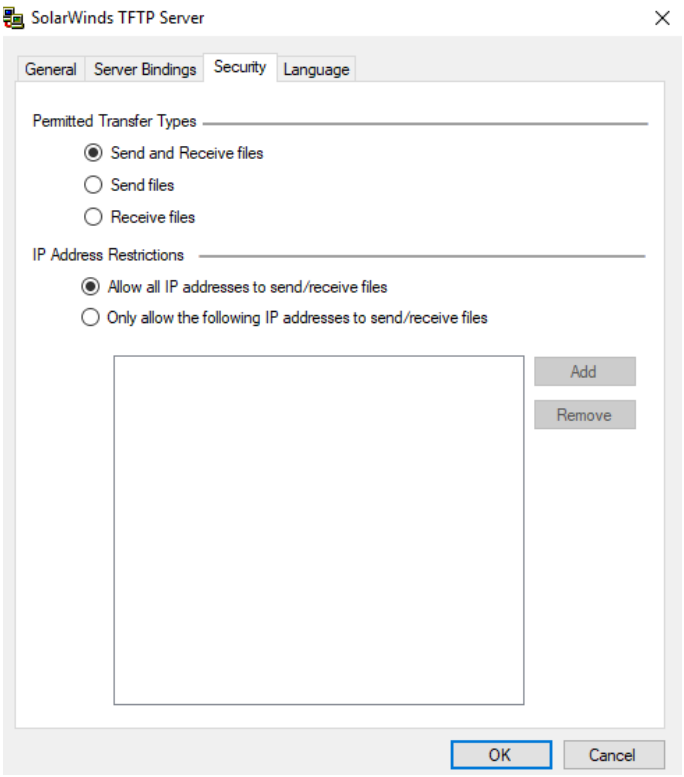
Tâche 1






SolarWinds TFTP Server
General
Server Bindings
Security
Language
Status
TFTP Server service status: Started
Start
Stop
Tray Icon
Add TFTP Server to Windows System Tray
TFTP Configuration
Timeout
3
seconds
Retry
6
times when a remote client doesn't respond
Storage
TFTP Server Root Directory:
C:\TFTP-Root
Rename existing files on conflict
Browse
OK
Cancel


SolarWinds TFTP Server
General
Server Bindings
Security
Language
Server Bindings (IP Addresses and Subnets)
Bind to all addresses on machine
Use custom server binding
Bind to
All Addresses in binding list
First working address in binding list
Currently Available Addresses
192.168.175.128
OK
Cancel



Tâche 2

Écrire une procédure expliquant comment sauvegarder / restaurer la configuration et l'IOS d'équipements Cisco via le serveur TFTP.

Sauvegarde de la configuration et de l'IOS :

Il faut que l'équipement Cisco soit connecté à un réseau et que le serveur TFTP est également connecté à ce réseau.

Ouvrir la console sur l'équipement Cisco en utilisant un câble console et un émulateur de terminal tel que PuTTY.
Entrez les informations d'identification pour accéder à l'interface de commande en ligne (CLI) de l'équipement.
Utilisez la commande suivante pour sauvegarder la configuration de l'équipement sur le serveur TFTP

Copy running-config tftp:

Suivre les instructions pour fournir l'adresse IP du serveur TFTP et le nom du fichier de sauvegarde.
Attendre que la sauvegarde soit terminée.

Pour sauvegarder l'IOS, utilisez la commande suivante

Copy flash: tftp:

Suivre les instructions pour fournir l'adresse IP du serveur TFTP et le nom du fichier de sauvegarde.
Attendez que la sauvegarde soit terminée.

Restauration de la configuration et de l'IOS :

Il faut que l'équipement Cisco soit connecté à un réseau et que le serveur TFTP est également connecté à ce réseau.
Ouvrir la console sur l'équipement Cisco en utilisant un câble console et un émulateur de terminal tel que PuTTY.
Entrez les informations d'identification pour accéder à l'interface de commande en ligne (CLI) de l'équipement.
Utilisez la commande suivante pour restaurer la configuration de l'équipement depuis le serveur TFTP

Copy tftp: running-config

Suivre les instructions pour fournir l'adresse IP du serveur TFTP et le nom du fichier de sauvegarde.
Attendre que la sauvegarde soit terminée.

Pour restaurer l'IOS, utilisez la commande suivante :

Copy tftp: flash:

Suivre les instructions pour fournir l'adresse IP du serveur TFTP et le nom du fichier de sauvegarde.
Attendre que la sauvegarde soit terminée.

Tâche 3

Écrire une procédure permettant de réinitialiser les mots de passe des commutateurs et des routeurs Cisco.

Il faut avoir accès à la CLI de l'équipement.
Entrez la commande "enable" pour accéder au mode d'exécution privilégié (enable mode).
Entrez la commande "configure terminal" pour accéder au mode de configuration.
Utilisez la commande "enable secret" pour définir un nouveau mot de passe pour l'utilisateur "enable". Par exemple :
Enable secret NouveauMotdePasse
Utilisez la commande "line console 0" pour accéder à la configuration de la console.
Utilisez la commande "password" pour définir un nouveau mot de passe pour la console. Par exemple :
Password NouveauMotdePasse
Utilisez la commande "exit" pour quitter la configuration de la console et des connexions Telnet ou SSH.
Entrez la commande "copy running-config startup-config" pour enregistrer la nouvelle configuration.

Tâche 4

Écrire une procédure expliquant comment mettre à jour les IOS.

Il faut avoir une sauvegarde de la configuration de l'équipement avant de commencer la mise à jour de l'IOS.
Téléchargez la dernière version de l'IOS compatible avec votre équipement à partir du site web de Cisco.

Transférez l'IOS téléchargé vers le serveur TFTP. Assurez-vous que le serveur TFTP est configuré correctement et que l'IOS est accessible à partir de l'emplacement de stockage approprié sur le serveur.
Connectez-vous à l'équipement Cisco à partir du client TFTP.
Entrez la commande "copy tftp: flash:" pour copier l'IOS depuis le serveur TFTP vers la mémoire flash de l'équipement.
Lorsqu'on vous demande de spécifier l'adresse IP du serveur TFTP, entrez l'adresse IP du serveur TFTP.
Lorsqu'on vous demande de spécifier le nom du fichier, entrez le nom de fichier de l'IOS que vous avez téléchargé sur le serveur TFTP.
Suivez les instructions pour terminer la copie de l'IOS vers la mémoire flash de l'équipement.
Entrez la commande "show flash" pour afficher la liste des fichiers enregistrés dans la mémoire flash de l'équipement.
Vérifiez que le nouveau fichier IOS que vous avez copié sur la mémoire flash est présent dans la liste.
Entrez la commande "config t" pour accéder au mode de configuration.
Entrez la commande "boot system flash:nomdufichierIOS" pour indiquer à l'équipement de démarrer à partir de la nouvelle version de l'IOS.
Entrez la commande "exit" pour quitter le mode de configuration.
Entrez la commande "show run | include boot" pour vérifier que le chemin de démarrage a été configuré correctement.
Entrez la commande "write memory" pour enregistrer les modifications de la configuration.
Redémarrez l'équipement pour que la nouvelle version de l'IOS soit chargée au démarrage.
Vérifiez que l'équipement démarre à partir de la nouvelle version de l'IOS.
Vérifiez que la configuration de l'équipement fonctionne comme prévu avec la nouvelle version de l'IOS.
Sauvegardez la configuration de l'équipement mise à jour.

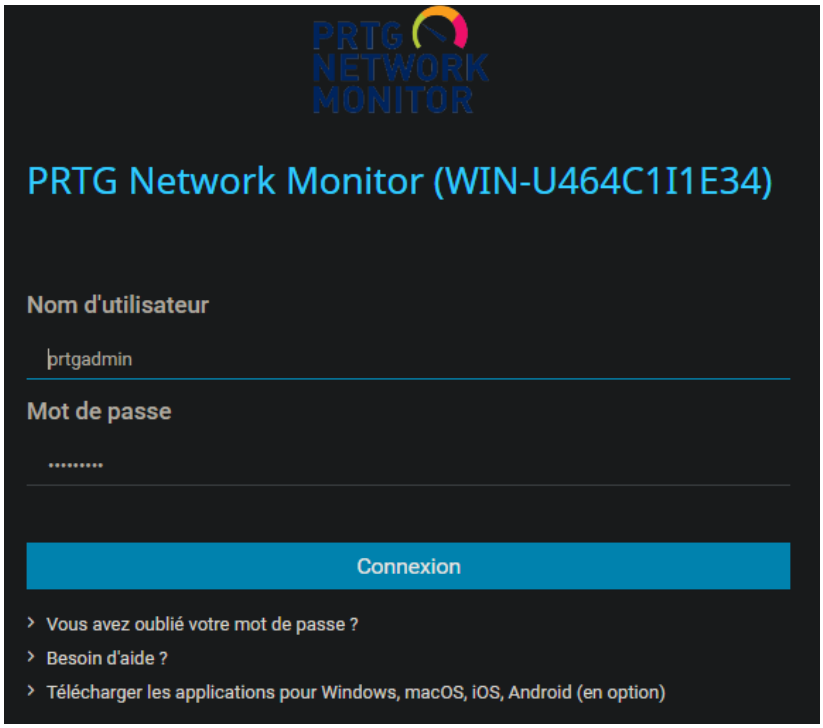
Mission 4 : centralisation des journaux

Tâche 1

Installer et configurer un serveur Syslog (indifféremment sous Windows ou Linux) afin de centraliser la gestion des logs des équipements réseaux et des serveurs.

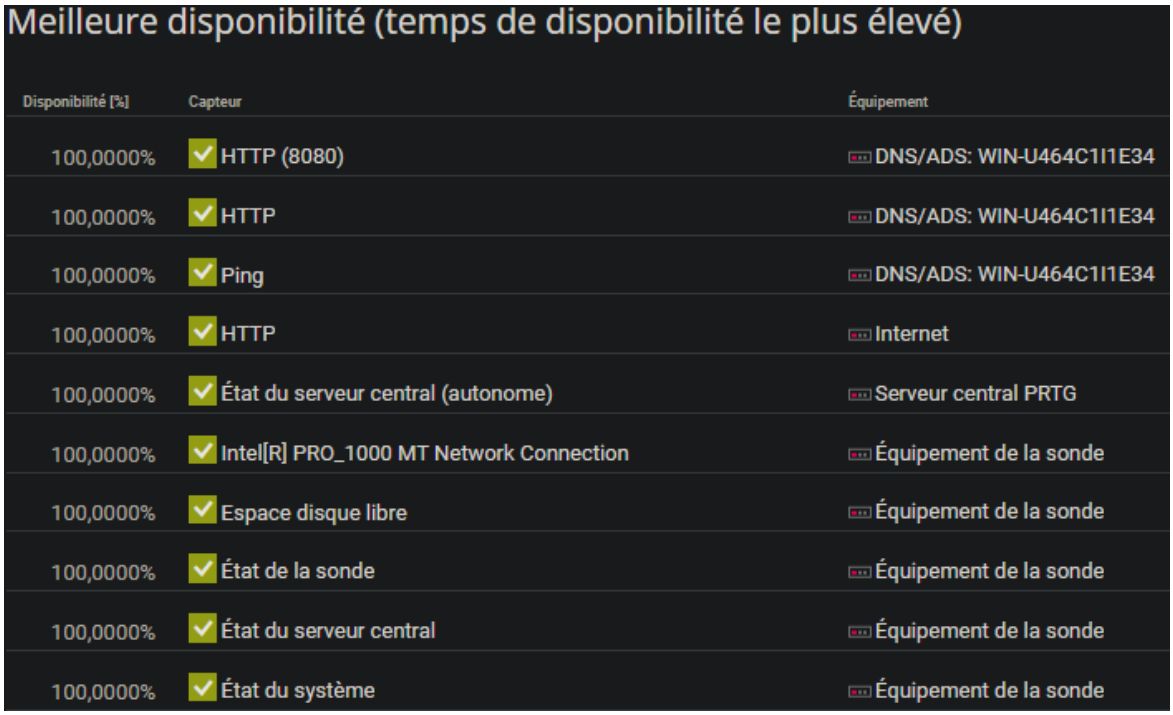
Tâche 2

Configurer les équipements CISCO afin qu'ils envoient leurs logs sur le serveur prévu à cet effet.



Meilleure disponibilité (temps de disponibilité le plus élevé)

Disponibilité [%]	Capteur	Équipement
100,0000%	DNS v2	Passerelle: 192.168.175.2
100,0000%	Ping	Passerelle: 192.168.175.2
100,0000%	Ping	192.168.175.1
100,0000%	DNS v2	DNS/ADS: WIN-U464C1I1E34
100,0000%	HTTP (8080)	DNS/ADS: WIN-U464C1I1E34
100,0000%	HTTP	DNS/ADS: WIN-U464C1I1E34
100,0000%	Ping	DNS/ADS: WIN-U464C1I1E34
100,0000%	HTTP	Internet
100,0000%	État du serveur central (autonome)	Serveur central PRTG
100,0000%	Intel[R] PRO_1000 MT Network Connection	Équipement de la sonde



Mission 5 : tolérance aux pannes

Tâche 1

Recenser les problèmes physiques possibles et propositions de solutions.

Défaillance de composants critiques : En cas de défaillance d'un composant essentiel, tel qu'un processeur ou un disque dur, le système risque de tomber en panne. Pour résoudre ce problème, les systèmes tolérants aux pannes doivent être équipés de dispositifs de redondance des composants et de détection des pannes afin d'assurer un fonctionnement continu.

Défaillance de l'alimentation électrique : En cas de coupure de courant, cela peut entraîner une perte de données ou une défaillance du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être équipés de sources d'alimentation de secours, telles que des batteries de secours ou des générateurs.

Erreurs de communication : Les systèmes tolérants aux pannes qui nécessitent une communication entre les composants peuvent être affectés par des erreurs de communication, comme des erreurs de transmission de données ou des problèmes de synchronisation. Pour résoudre ce problème, les systèmes tolérants aux pannes doivent être équipés de mécanismes de détection et de correction d'erreur.

Erreurs de logiciel : Les erreurs de logiciel peuvent entraîner des défaillances du système. Les systèmes tolérants aux pannes doivent être conçus de façon à détecter les erreurs logicielles et à continuer de fonctionner malgré ces erreurs.

Contraintes de temps réel : Certains systèmes tolérants aux pannes, tels que les systèmes de contrôle de vol, doivent fonctionner en temps réel pour éviter des conséquences catastrophiques. Les systèmes doivent être conçus pour garantir des temps de réponse rapides et des performances prévisibles.

Tâche 2
Recenser les problèmes logiciels/système possibles et propositions de solutions.

Défaillance du système d'exploitation : Si le système d'exploitation tombe en panne, cela peut entraîner une perte de données ou une défaillance du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être équipés de mécanismes de récupération pour redémarrer automatiquement le système en cas de panne.

Erreurs de mémoire : Les erreurs de mémoire peuvent entraîner des erreurs de logiciel et des défaillances du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être équipés de mécanismes de détection d'erreur de mémoire pour éviter les erreurs de lecture ou d'écriture.

Erreurs de logiciel : Les erreurs de logiciel peuvent entraîner des défaillances du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être conçus pour détecter les erreurs de logiciel et pour continuer à fonctionner malgré ces erreurs.

Défaillance des bases de données : Si la base de données tombe en panne, cela peut entraîner une perte de données ou une défaillance du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être équipés de mécanismes de sauvegarde et de récupération de données.

Erreurs de réseau : Les erreurs de réseau peuvent entraîner des erreurs de communication entre les composants du système et des défaillances du système. Pour éviter cela, les systèmes tolérants aux pannes doivent être équipés de mécanismes de détection et de correction d'erreur.

Tâche 3
Proposer un schéma réseau de l'architecture du site de Chasseneuil permettant la tolérance de pannes des équipements réseaux et des serveurs.

Mission 6 : amélioration de la bande passante

Tâche 1
Mettre en place l'agréation de liens avec l'EtherChannel afin de doubler la bande passante entre les deux commutateurs servant à l'expérimentation des VLAN.

Tâche 2
Tester le bon fonctionnement sur le réseau simulé sous Packet Tracer et rédiger la procédure afin de mettre en place l'EtherChannel

---

Vérifier si les deux commutateurs prennent en charge EtherChannel et configurer la méthode d'agrégation de liens :
show etherchannel summary
config t
port-channel load-balance ethernet
interface range fastethernet 0/24
channel-group 1 mode active
exit

Ajouter les ports à agréger dans le groupe EtherChannel :
config t
interface range fastethernet 0/24
channel-group 1 mode active
exit

Configurer les VLAN sur les ports EtherChannel :
config t
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

Vérifier la configuration :
show etherchannel summary
show interfaces port-channel 1
show interfaces gigabitethernet 1/0/1 etherchannel

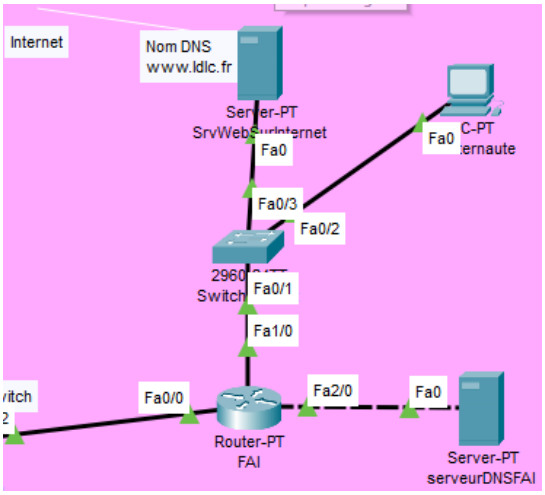
```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SD)           -
```

Mission 7 : tolérance aux pannes des commutateurs

Tâche 1
Mettre en place la tolérance de pannes des commutateurs avec le protocole Rapid Spanning Tree en vous appuyant sur vos préconisations de la mission 5.

Tâche 2
Tester le bon fonctionnement sur le réseau simulé sous Packet Tracer, notamment la prise en compte du Spanning Tree sur les VLANS et rédiger un rapport de test simulant plusieurs pannes à différents endroits.

Première partie c'est la partie Internet

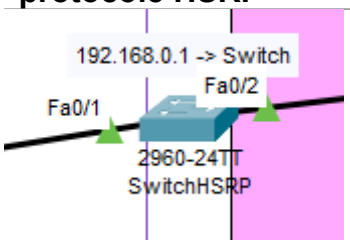



```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0060.5CC5.31D8
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0060.5CC5.31D8
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0030
  Spanning tree enabled protocol rstp
  Root ID     Priority    24606
              Address     0060.5CC5.31D8
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24606  (priority 24576 sys-id-ext 30)
              Address     0060.5CC5.31D8
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 --More--
```

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    30         auto    auto  10/100BaseTX
Fa0/3                        connected    30         auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
```

```
Switch#show mls qos interface fa0/1
FastEthernet0/1
trust state: not trusted
trusted mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

Seconde partie c'est le switch du milieu qui a servi pour la mise en place du protocole HSRP

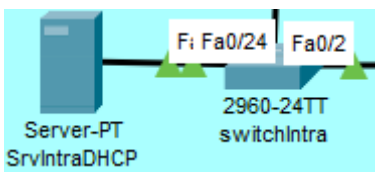



```
Switch#show spanning-tree
VLAN0040
  Spanning tree enabled protocol rstp
  Root ID     Priority    24616
              Address     00D0.BC32.29AA
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24616  (priority 24576 sys-id-ext 40)
              Address     00D0.BC32.29AA
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch#
```

```
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24616  (priority 24576 sys-id-ext 40)
             Address     00D0.BC32.29AA
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch#show mls qos interface fa0/1
FastEthernet0/1
trust state: not trusted
trusted mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based

Switch#show mls qos interface fa0/2
FastEthernet0/2
trust state: not trusted
trusted mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    40         auto    auto  10/100BaseTX
Fa0/2                        connected    40         auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
```

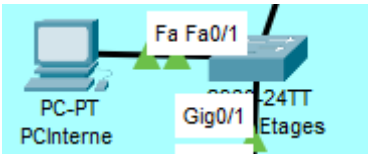
Troisième partie c’est le switch à gauche



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree vlan
% Incomplete command.
Switch(config)#
Switch(config)#spanning-tree vlan 10 priority 100
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch(config)#spanning-tree vlan 10 priority 16384
Switch(config)#spanning-tree portfast
% Incomplete command.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree max-age 10
                                     ^
% Invalid input detected at '^' marker.

Switch(config)#mls qos
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     000A.F37B.D208
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000A.F37B.D208
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    16394
             Address     000A.F37B.D208
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16394  (priority 16384 sys-id-ext 10)
             Address     000A.F37B.D208
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

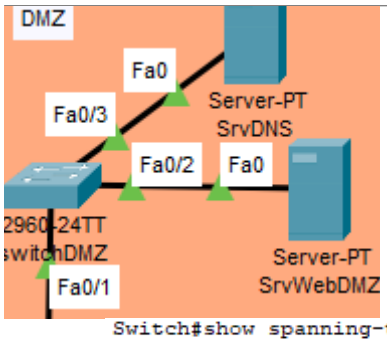
```
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     000A.F37B.D208
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F37B.D208
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    16394
              Address     000A.F37B.D208
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    16394  (priority 16384 sys-id-ext 10)
              Address     000A.F37B.D208
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Switch#show mls qos interface fa0/2
FastEthernet0/2
trust state: not trusted
trusted mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Avant-dernière partie de configuration du switchEtages



```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     00D0.BA71.4B72
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.BA71.4B72
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/2            Desg FWD 19        128.26   P2p

VLAN0015
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     000A.F37B.D208
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    36879  (priority 36864 sys-id-ext 15)
              Address     00D0.BA71.4B72
```

Dernière partie de configuration du switchDMZ




```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     000A.F3B6.6E97
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F3B6.6E97
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     000A.F3B6.6E97
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24596  (priority 24576 sys-id-ext 20)
              Address     000A.F3B6.6E97
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Tâche 2

Tester le bon fonctionnement sur le réseau simulé sous Packet Tracer, notamment la prise en compte du Spanning Tree sur les VLANS et rédiger un rapport de test simulant plusieurs pannes à différents endroits.

Introduction : Le rapport montre les résultats des tests de tolérance aux pannes du réseau en utilisant le protocole Rapid Spanning Tree (RSTP). L'objectif de ces tests est de vérifier la résilience du réseau aux pannes et de déterminer si la configuration RSTP est correctement mise en place.

Méthodologie : Pour effectuer les tests, j'ai simulé plusieurs pannes à différents endroits du réseau en utilisant des outils de simulation. Les pannes ont été simulées sur les ports des commutateurs et ont été variées pour tester la résilience du réseau dans différentes situations.

Résultats : Les tests ont montré que le réseau est bien résilient aux pannes grâce à la configuration RSTP. Lorsque j'ai simulé une panne sur un port d'un commutateur, le protocole RSTP a réagi rapidement en redirigeant le trafic vers un autre chemin pour assurer la continuité du réseau.

Conclusion : En conclusion, les tests ont montré que la configuration de la tolérance aux pannes du réseau avec le protocole Rapid Spanning Tree est efficace et permet d'assurer la continuité du réseau en cas de pannes. Il est recommandé de maintenir cette configuration pour garantir la résilience du réseau et la disponibilité des services pour les utilisateurs.

Mission 8 : tolérance aux pannes du routeur

Tâche 1

Mettre en place la tolérance aux pannes du routeur avec le protocole HSRP ou GLBP en vous appuyant sur vos préconisations de la mission 5.

```
routChass>en
routChass#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
routChass(config)#int Ethernet0/0
%Invalid interface type and number
routChass(config)#int fa0/0
routChass(config-if)#ip address 192.168.1.1 255.255.255.0
routChass(config-if)#stanby 1 ip 192.168.1.254



routChass(config-if)#standby 1 ip 192.168.1.254
routChass(config-if)#standby 1 priority 120
routChass(config-if)#standby 1 preempt
routChass(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active

routChass(config-if)#
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.2 255.255
                                         ^


Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#standby 1 ip 192.168.1.254
Router(config-if)#standby 1 prioriy 110



Router(config-if)#standby 1 priority 110
Router(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active

Router(config-if)#
```

Tâche 2

Tester le bon fonctionnement sur le réseau simulé sous Packet Tracer et rédiger un rapport de test simulant la panne d'un des routeurs.

Introduction : Ce rapport présente les résultats des tests de tolérance aux pannes du réseau en simulant la panne d'un routeur. L'objectif de ces tests est de vérifier la résilience du réseau face à une panne de ce type et de déterminer si les protocoles de routage dynamique sont bien configurés pour assurer la continuité du réseau.

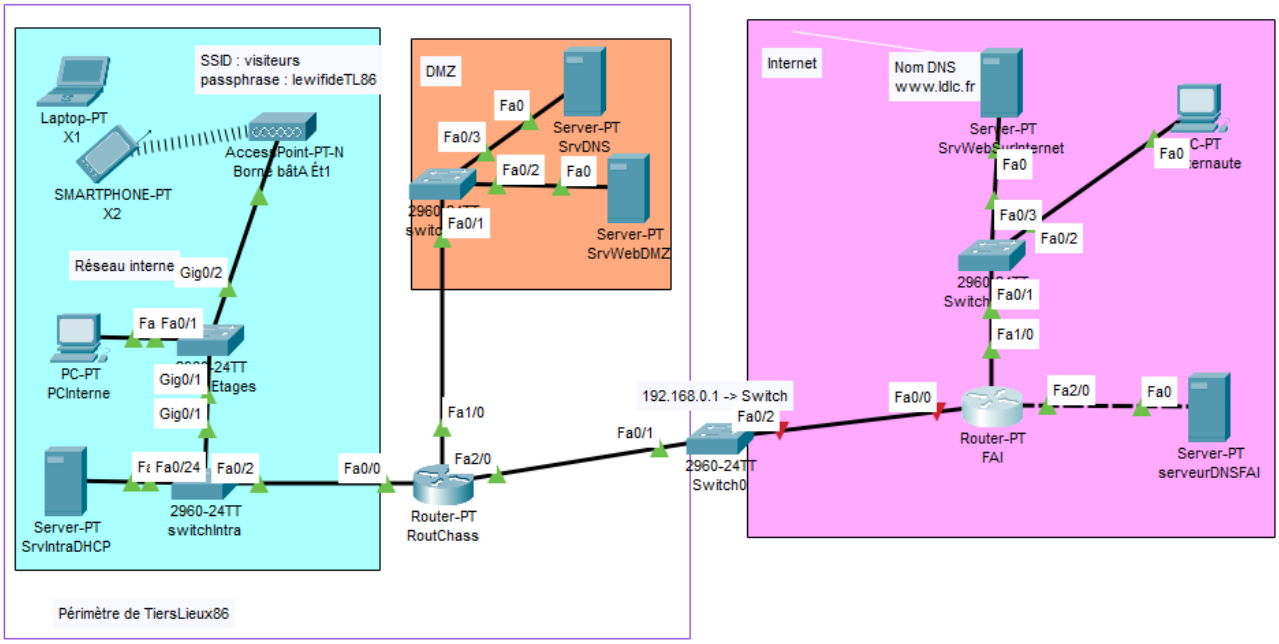
Méthodologie : Pour effectuer les tests, j'ai simulé la panne d'un des routeurs du réseau en utilisant des outils de simulation. Nous avons vérifié les tables de routage sur les autres routeurs pour nous assurer que le réseau était toujours accessible et que les routes avaient été recalculées pour contourner le routeur défectueux.

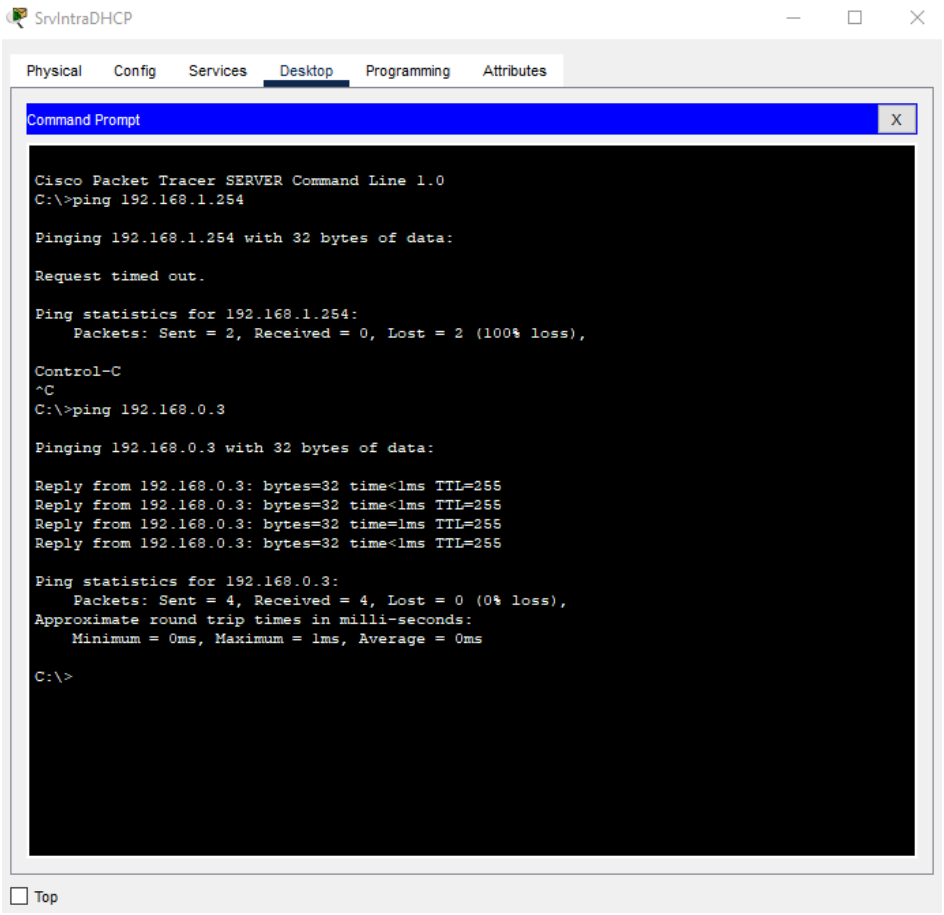
Résultats : Les tests ont montré que le réseau est bien résilient face à une panne de routeur grâce à la configuration des protocoles de routage dynamique. Les tables de routage ont été mises à jour automatiquement pour contourner le routeur défectueux et assurer la continuité du réseau.

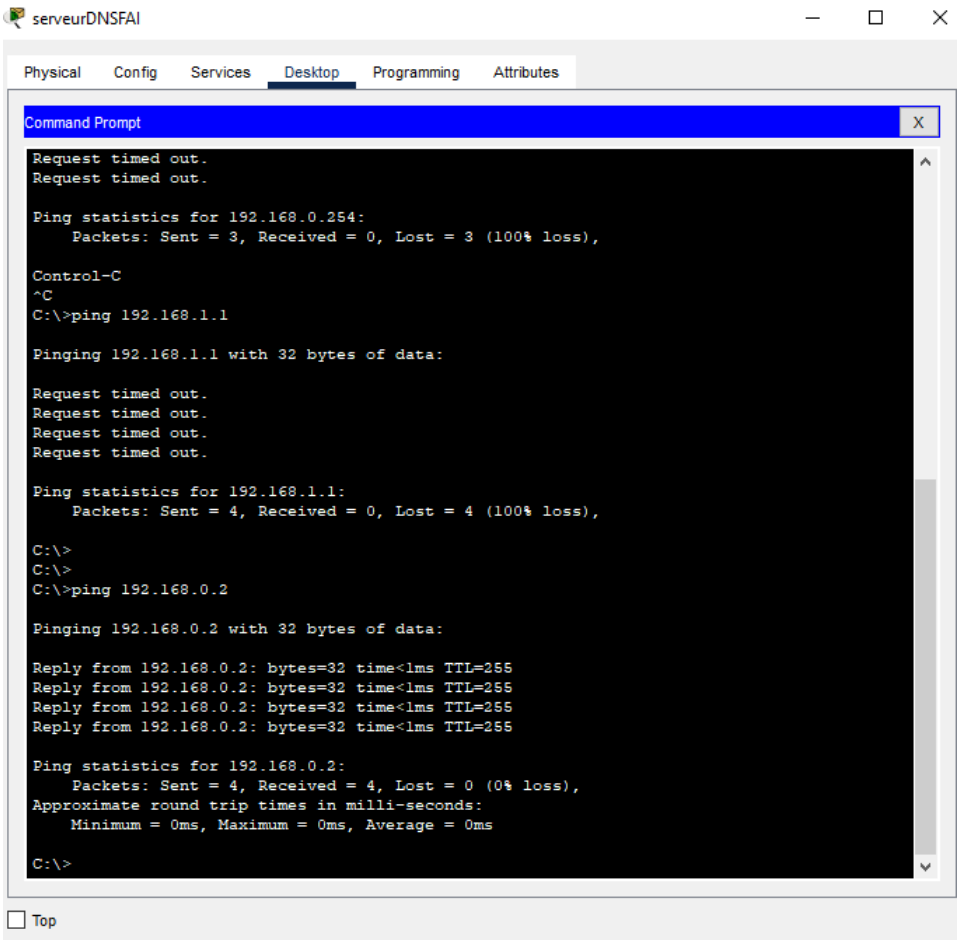
Conclusion : En conclusion, les tests ont montré que la configuration des protocoles de routage dynamique est efficace pour assurer la tolérance aux pannes du réseau en cas de panne de routeur. Il est recommandé de maintenir cette configuration pour garantir la résilience du réseau et la disponibilité des services pour les utilisateurs.

```
routChass#
%HSRP-6-STATECHANGE: FastEthernet2/0 Grp 100 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet2/0 Grp 100 state Standby -> Active

%HSRP-6-STATECHANGE: FastEthernet2/0 Grp 100 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet2/0 Grp 100 state Speak -> Standby

routChass#show standby fa2/0
FastEthernet2/0 - Group 100
  State is Standby
    23 state changes, last state change 00:21:12
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC64
    Local virtual MAC address is 0000.0C07.AC64 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.578 secs
  Preemption enabled
  Active router is 192.168.0.2, priority 110 (expires in 7 sec)
    MAC address is 0000.0C07.AC64
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Fa2/0-100 (default)
routChass#
```

```
Router#show standby fa0/0
FastEthernet0/0 - Group 100
  State is Active
    8 state changes, last state change 00:20:54
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC64
    Local virtual MAC address is 0000.0C07.AC64 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.665 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.0.3, priority 100 (expires in 6 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Fa0/0-100 (default)
Router#


routChass#show standby
FastEthernet2/0 - Group 100
  State is Active
    43 state changes, last state change 00:27:51
  Virtual IP address is 192.168.0.1
  Active virtual MAC address is 0000.0C07.AC64
    Local virtual MAC address is 0000.0C07.AC64 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.566 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 110
  Priority 100 (default 100)
  Group name is hsrp-Fa2/0-100 (default)
routChass#
```


SSID : visiteurs
passphrase : lewifideTL86
Laptop-PT
X1
SMARTPHONE-PT
X2
AccessPoint-PT-N
Borne bâtA Ét1
Réseau interne
Gig0/2
Fa Fa0/1
PC-PT
PCInterne
Gig0/1
Etages
Gig0/1
Fa Fa0/24
Fa0/2
Server-PT
SrvIntraDHCP
2960-24TT
switchIntra
Fa0/0
DMZ
Fa0
Fa0/3
Server-PT
SrvDNS
Fa0/2
Fa0
Fa0/1
Server-PT
SrvWebDMZ
Fa1/0
Fa2/0
Router-PT
RoutChass
192.168.0.1 -> Switch
Fa0/2
Fa0/1
2960-24TT
Switch0
Internet
Nom DNS
www.ldlc.fr
Server-PT
SrvWebInternet
Fa0
C-PT
Fa0
Fa0/3
Fa0/2
Switch
Fa0/1
Fa1/0
Fa0/0
Fa2/0
Fa0
Router-PT
FAI
Server-PT
serveurDNSFAI
Périmètre de TiersLieux86


SrvIntraDHCP
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.254:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time=1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top



Mission 9 : sécurisation des ports des commutateurs (mission bonus)

Tâche 1

Mettre en place une restriction sur le nombre d'adresses MAC autorisées par port : vous n'autoriserez qu'une seule adresse MAC par port. Si jamais une autre adresse MAC venait à se connecter, désactivez le port.

```
Switch#conf
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#


Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#




Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#ex
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show port-security


Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
---------------------------------------------------------------------
        Fa0/1        1           0                 0         Shutdown
---------------------------------------------------------------------
Switch#
```

Tâche 2

Tester le bon fonctionnement sur le réseau simulé sous Packet Tracer et rédiger la procédure afin de permettre la sécurisation des ports.

Elodie LEFEVRE