

# Tutorial Cisco Catalyst 3500 Series

Configuration de VLANs niveau 2

Nolmë Informatique

**NOLMË INFORMATIQUE**

16 novembre 2010

Créé par : Anthony Theuray

Version : 1.4 0

# ***AVERTISSEMENT***

---

LES EXPERIENCES, TESTS ET CONFIGURATIONS PRESENTEES DANS CE DOCUMENT SONT PROPOSES A TITRE INFORMATIF ET EDUCATIF AFIN D'EXPLIQUER SIMPLEMENT CERTAINS CONCEPTS DE BASE. TOUTE UTILISATION EN DEHORS DE CE CADRE EST DE LA RESPONSABILITE DU OU DES PERSONNES REALISANT CES TESTS.

NOLMÈ INFORMATIQUE DECLINE TOUTE RESPONSABILITE QUANT A L'UTILISATION EVENTUELLES DE TOUTE INFORMATION CONTENUE DUDIT DOCUMENT ET DES CONSEQUENCES DE SON UTILISATION.

LES TENTATIVES NON AUTORISEES DE CHARGEMENT OU DE MODIFICATION DE L'INFORMATION DANS CE DOCUMENT SONT STRICTEMENT INTERDITES ET PEUVENT TOMBER SOUS LE COUP DES LOIS SUR LA FRAUDE INFORMATIQUE AINSI QUE D'AUTRES LOIS FEDERALES ET PROVINCIALES.

TOUTE L'INFORMATION CONTENUE DANS CE DOCUMENT EST PROTEGEE PAR UN COPYRIGHT DE NOLMÈ INFORMATIQUE OU DE L'UNE DE SES COMPAGNIES. CETTE INFORMATION NE PEUT PAS ETRE MODIFIEE D'UNE MANIERE QUELCONQUE SANS LE CONSENTEMENT ECRIT PREALABLE DE NOLMÈ INFORMATIQUE.

Nolmè Informatique



# SOMMAIRE

## Contenu

<b>I. INTRODUCTION</b> .....	<b>4</b>
A. Présentation .....	4
B. Contexte général .....	4
C. Contexte spécifique .....	4
D. Prérequis techniques .....	4
<b>II. MATERIEL UTILISE</b> .....	<b>5</b>
A. Matériel utilisé .....	5
B. Pré-configuration .....	5
1. PRE-CONFIGURATION MATERIELLE .....	5
2. PRE-CONFIGURATION LOGICIELLE .....	5
3. PRE-CONFIGURATION DU SWITCH .....	6
<b>III. EXEMPLES D'APPLICATION</b> .....	<b>7</b>
A. Sécurité .....	7
B. Optimisation .....	7
<b>IV. OBJECTIF(S)</b> .....	<b>8</b>
A. Projet .....	8
B. Analyse du projet .....	8
<b>V. CONFIGURATION DE L'ARCHITECTURE SIMPLIFIEE</b> .....	<b>10</b>
A. Vérifications .....	10
B. Création des VLANs .....	10
C. Attribution des ports .....	11
D. Tests de la configuration .....	12
1. CONNECTIVITE SERVEUR / UTILISATEUR .....	12
2. CONNECTIVITE SERVEUR / INFORMATIQUE .....	13
3. CONNECTIVITE INFORMATIQUE / UTILISATEUR .....	13
4. PREMIERES CONCLUSIONS .....	13
<b>VI. CONFIGURATION DE L'ARCHITECTURE COMPLETE</b> .....	<b>14</b>
A. Vérifications .....	14
B. Création des VLANs .....	14
C. Attribution des ports .....	14
D. Tests de la configuration .....	16
<b>VII. CONFIGURATION COMPLETE (CLI)</b> .....	<b>17</b>
A. Création des VLANs .....	17
B. Attribution des ports .....	17
<b>VIII. ANNEXES</b> .....	<b>19</b>
A. Glossaire .....	19
B. Logiciels tiers .....	20
C. Autres annexes .....	20

# I. Introduction

## A. Présentation

Les membres de la société Nolmë Informatique sont des professionnels qui, au travers de leur expérience personnelle ou professionnelle, partagent leurs connaissances au sein de la communauté.

## B. Contexte général

Le matériel réseau se diversifie de plus en plus avec des fonctions de plus en plus complexes. Entre les versions anglaises et les nouvelles fonctionnalités, il devient parfois difficile de s'y retrouver.

Au travers ce document, vous apprendrez à configurer des produits réseaux précis afin de pouvoir être capable de reproduire et créer vos propres configurations de manière efficace et sécurisée. Vous comprendrez aussi certains aspects et contraintes souvent liés à la technologie.

Ce document n'est pas figé, au travers de vos commentaires et remarques il évoluera avec le temps afin de le rendre encore plus complet.

En espérant qu'il répondre à vos besoins et interrogations sur le sujet.

Bonne configuration,

L'équipe Nolmë Informatique.

## C. Contexte spécifique

Afin d'isoler certains segments d'un réseau informatique pour plus de sécurité ou pour optimiser la bande passante, il peut être intéressant de créer des VLANs.

Ce document aborde au travers d'un Switch de niveau 2, les VLANs de même niveau à savoir les VLANs par port.

## D. Prérequis techniques

Afin d'assimiler la majeure partie de ce document, certains prérequis peuvent être nécessaires. Si le glossaire en fin de document ne répondait pas à vos interrogations, nous vous conseillons de vous documenter sur les sujets en question avant de poursuivre la lecture.

Parmi les prérequis technique :

- Maitriser les bases du réseau (plages IP, routage)

## II. Matériel utilisé

### A. Matériel utilisé

Le matériel utilisé pour cette présentation est :

- Cisco Catalyst 3500 XL Series avec le firmware 12.0(5)WC17 – C3500XL-C3H2S-M.

Le matériel complémentaire abordé pour ce tutorial est :

- Netgear FVS318G servant de passerelle Internet.

Pour les tests et mesures les appareils et ordinateurs suivants ont été utilisés :

- Ordinateur fixe PackardBell iMedia, Windows 7 Pro Fr.
- Ordinateur portable NEC Versa P570, Windows 7 Pro Fr.

Le raccordement à Internet est effectué via :

- Ligne ADSL Orange 18 Méga.

### B. Pré-configuration

Avant de démarrer sur ce tutoriel, une pré-configuration peut s'avérer nécessaire. Sa légitimité tient au fait que certains réglages peuvent avoir été abordés dans d'autres tutoriaux et que ce document veuille se focaliser plus précisément sur un point unique.

#### 1. Pré-configuration matérielle

Le matériel suivant est supposé branché, mis à jour et accessible via un navigateur web :

- Switch Cisco Catalyst 3500 XL Series branché avec l'adresse IP par défaut 172.16.1.10.
- Netgear FVS318G avec l'adresse IP par défaut 172.16.1.1.
- Ordinateur fixe PackardBell iMedia
  - Désigné par PC\_ADMIN.
  - Adresse IP: 172.16.1.200.
- Ordinateur portable NEC Versa P570
  - Désigné par PC\_TEST.
  - Adresse IP: 172.16.1.100.

**Attention** : vous devez spécifier explicitement l'adresse IP du Switch si vous connectez un routeur avec le DHCP active sous peine de voir son IP modifiée automatiquement.

#### 2. Pré-configuration logicielle

Pour pouvoir administrer le Switch via une interface graphique, il faut au préalable télécharger le « Cisco Network Assistant » (voir annexe).

Pour télécharger « Cisco Network Assistant », vous devez être en possession d'identifiants Cisco. Les revendeurs et ingénieurs certifiés disposent normalement tous de cet accès.

La machine virtuelle Java doit être installée sur l'ordinateur exécutant « Cisco Network Assistant ». Pour ce tutorial, nous avons utilisé la version 6 Update 22.

### 3. Pré-configuration du Switch

Afin d'utiliser correctement le Switch il faut tout d'abord faire un Reset Usine du Switch. Pour ce faire il faut lancer un logiciel comme HyperTerminal (9600, 8, aucun, 1, aucun) :

```
Switch_3500XL>en  
Password:  
Switch_3500XL#
```

Ensuite il suffit de taper la commande **write erase** :

```
Switch_3500XL#write erase  
Erasing the nvram filesystem will remove all files! Continue? [confirm]y[OK]  
Erase of nvram: complete  
Switch_3500XL#  
Switch_3500XL#reload  
System configuration has been modified. Save? [yes/no]: n
```

*Attention* : Ne pas sauvegarder la configuration ici, sinon le Switch ne sera pas remis en configuration usine !

```
Proceed with reload? [confirm]y
```

```
2w0d: %SYS-5-RELOAD: Reload requested
```

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)  
Compiled Mon 22-Jul-02 18:57 by antonino  
WS-C2950G-12-EI starting...
```

```
32K bytes of flash-simulated non-volatile configuration memory.  
Base ethernet MAC Address: 00:05:DC:C9:79:00  
Motherboard assembly number: 73-5781-08  
Motherboard serial number: FAB0515A069  
Model revision number: 02  
Model number: WS-C2950-24  
System serial number: FAB0517Q00B
```

```
--- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].  
Continue with configuration dialog? [yes/no]: y
```

Taper "y" pour lancer l'assistant de configuration et donner une IP au Switch.

### III. Exemples d'application

Cette section vous présente quelques-uns des exemples d'application du matériel. Bien entendu, il existe bien plus de possibilités qui ne dépendent généralement que de votre perception d'un problème donné.

Néanmoins, vous pourrez comprendre comment s'architecture les matériels réseaux entre eux.

#### A. Sécurité

Les VLANs peuvent être utilisés afin de cloisonner 'physiquement' des parties d'un réseau informatique pour des raisons de sécurité.

#### B. Optimisation

Les VLANs peuvent être utilisés pour optimiser la bande passante d'un Switch.

## IV. Objectif(s)

Au cours de ce document vous apprendrez à maîtriser différents aspects du ou des produits présentés. Parmi ces compétences, vous serez capables de :

- Créer des VLANs de niveau 2
- Isoler des segments du réseau local

### A. Projet

Un client souhaite différencier les différents pôles de son entreprise. Le découpage pourrait ressembler à ceci :

- Pôle utilisateur
- Pôle informatique
- Serveurs de production

Après discussion avec le client, il nous indique les règles de visibilité entre les groupes.

Le pôle utilisateur doit accéder aux serveurs et à Internet tout comme le pôle informatique. Par contre le pôle utilisateur et le pôle informatique ne doivent pas se voir.

### B. Analyse du projet

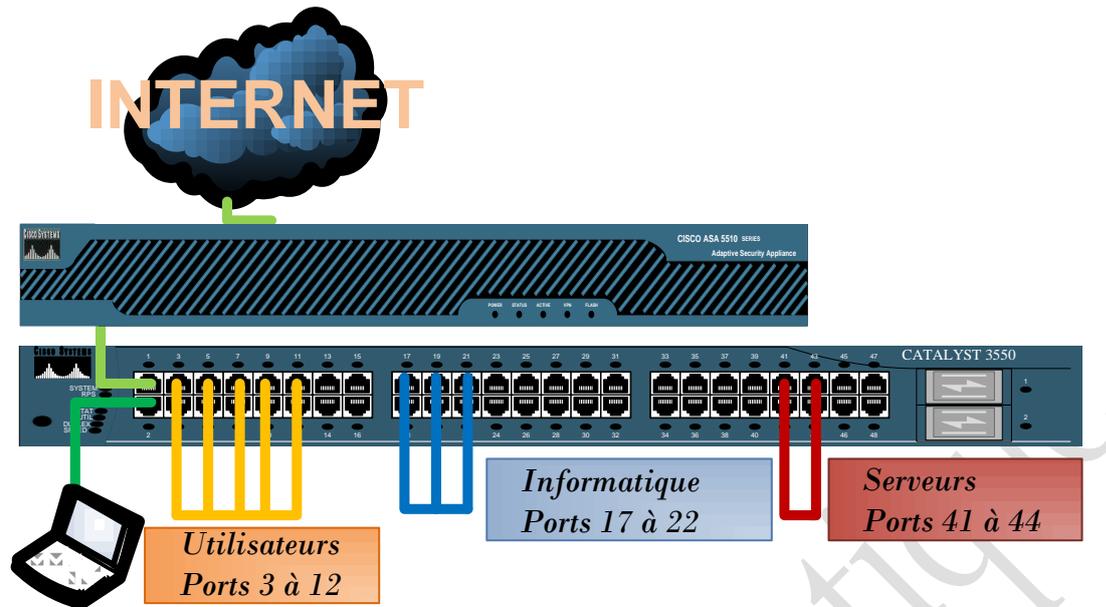
La représentation des besoins du client se traduit par le tableau suivant.

Tableau 1 - Visibilité des groupes

	Utilisateurs	Informatique	Serveurs	Internet
Utilisateurs	X		X	X
Informatique		X	X	X
Serveurs	X	X	X	X
Internet	X	X	X	X

Basé sur le nombre de machines dans chaque groupe, la composition du réseau peut être établi.

Figure 1 - Configuration physique des ports sur le Switch



**Attention :** Le bon brassage du réseau est un critère essentiel pour le bon fonctionnement des VLANs. Votre schéma doit donc être aussi précis que possible pour éviter toute erreur de relecture.

**Attention :** Si vos VLANs ont des vocations de cloisonnement et de sécurité, il est indispensable d'en protéger l'accès physique (aussi bien que l'accès web). En effet, une personne mal intentionnée pourrait déplacer un simple câble et donner accès à des ressources normalement non disponibles.

**Solution :** Il est possible de restreindre une adresse MAC à certains ports via le menu Configure->Switching->MAC Address.

## V. Configuration de l'architecture simplifiée

### A. Vérifications

Les menus peuvent bien entendu varier en fonction de la langue utilisée, de la version du produit ou bien du firmware. Il suffit généralement de regarder à proximité pour trouver l'option désirée.

Votre ordinateur est connecté au Switch. Cisco Network Assistant est en fonctionnement et est connecté aussi sur le Switch. Vous devez donc retrouver cette configuration dans le Front Panel View (Monitor -> Views -> Front Panel View). Si vous avez branché déjà branché le routeur, le port n°1 doit aussi être vert.

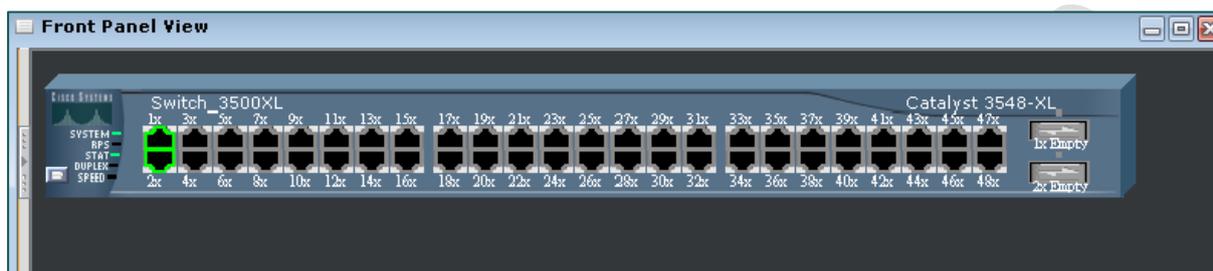


Figure 2 - front panel view, vérification de la connectique

### B. Création des VLANs

Maintenant que les besoins sont définis, on peut créer les premiers VLANs.

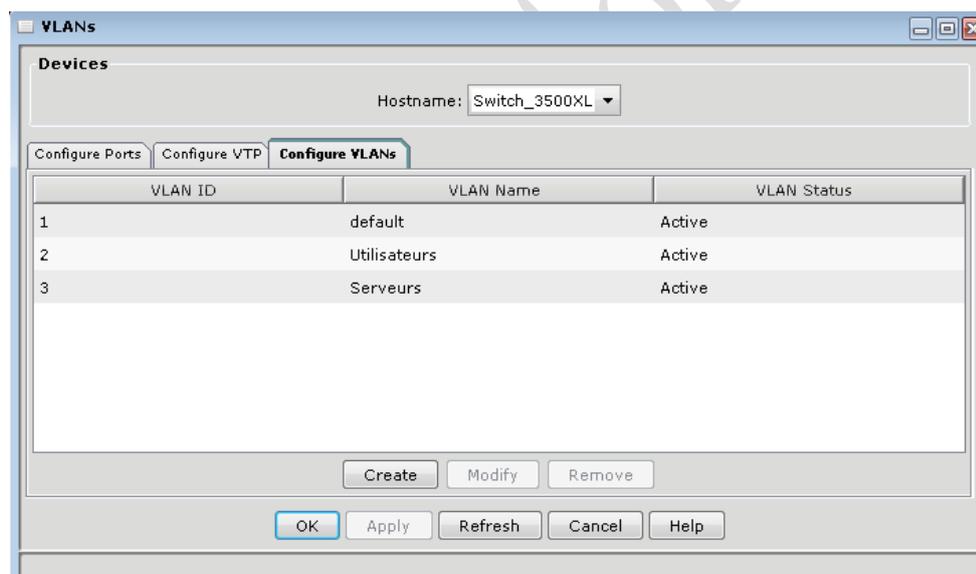


Figure 3 - Création des VLANs

Les numéros de VLAN ID sont fixés arbitrairement et leur nom (VLAN Name) est présenté pour notre bonne lecture et compréhension.

**Remarque :** On constate qu'aucun VLAN n'a été créé pour la division informatique car ils vont utiliser le VLAN n°1 déjà créé. Beaucoup de périphériques réseaux ne sont pas conçus pour être administrés sur un VLAN différent du n°1.

## C. Attribution des ports

Maintenant que les VLANs sont créés d'un point de vue logique, il faut les assigner aux différents ports du Switch.

**Rappel :** Votre schéma initial est crucial dans cette étape. Prenez le temps de l'étudier. Un VLAN prend 5 min à créer mais parfois plusieurs heures à penser.

**Attention :** Si l'ordinateur de configuration se trouve sur un port qui sera assigné à un VLAN différent de celui d'administration, vous perdrez la main sur le Switch. Si aucun port n'est défini pour le VLAN 1, il faudra alors faire un Reset usine.

Pour chacun des ports il faut lui assigner le VLAN ID qui lui correspond :

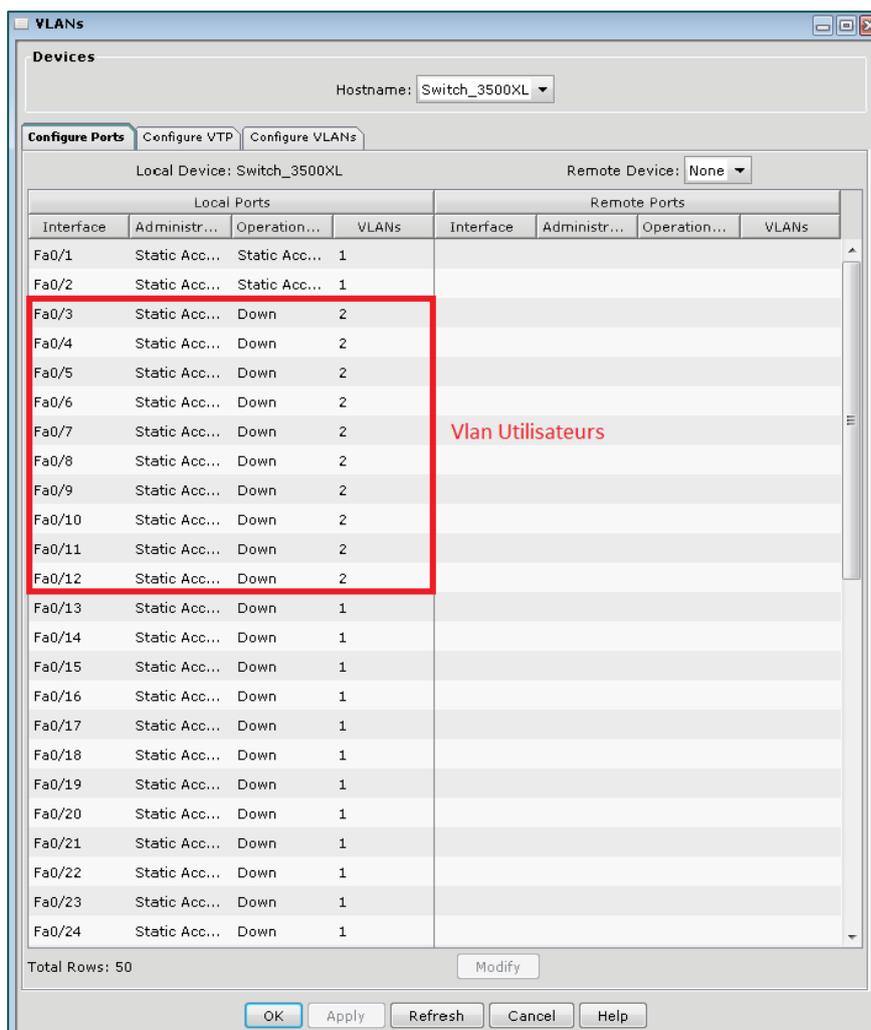


Figure 4 - Attribution des ports 1 à 24

**Astuce :** vous pouvez utiliser la touche **MAJ** pour sélectionner plusieurs ports.

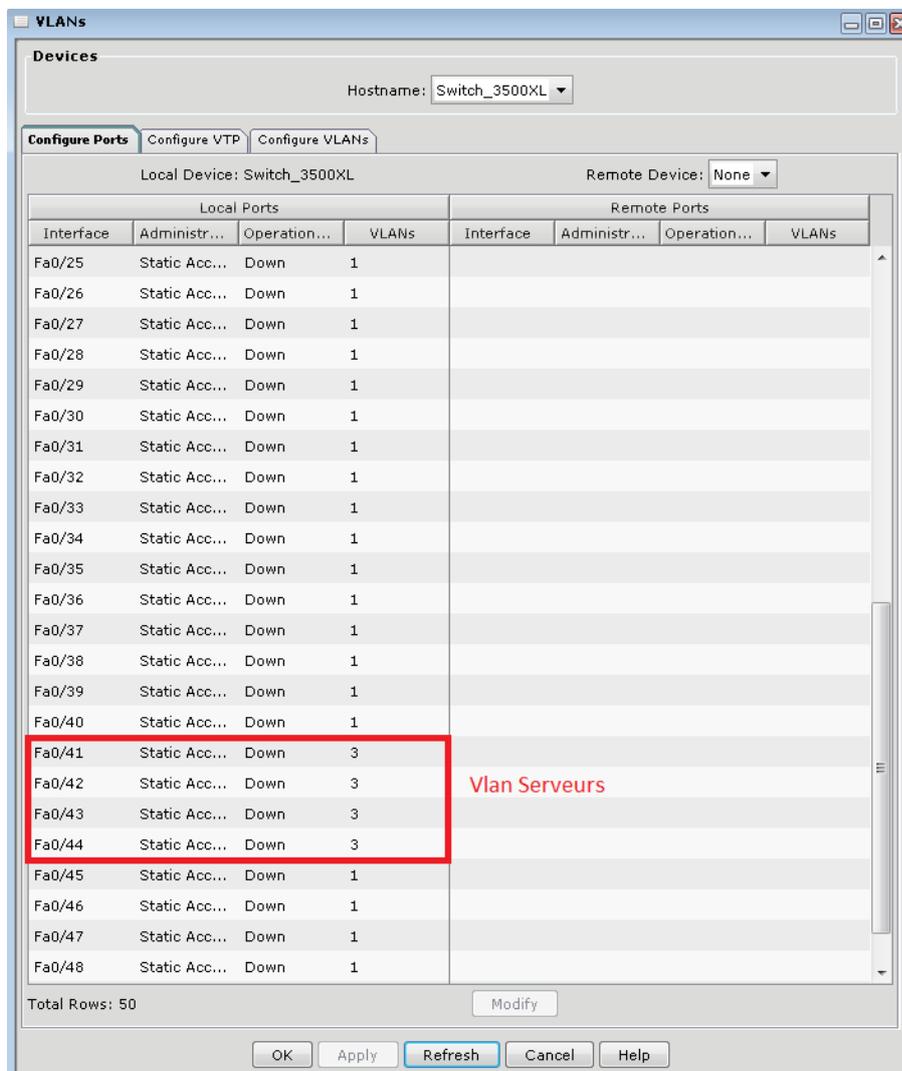


Figure 5 - Attribution des ports 25 à 48

## D. Tests de la configuration

**Note :** Avant tout test il est préférable de s'assurer que les différents ordinateurs utilisés pour tester la configuration soit bien configurés et puissent se 'Pinger' sans problème.

Assurez-vous dans un premier temps qu'au sein de chaque groupe, les machines se 'Ping' librement.

**Rappel :** Pour tester la commande 'Ping', il est préférable d'ouvrir une console soit par le menu Démarrer -> Exécuter -> cmd.exe soit par le menu Démarrer -> Tous les programmes -> Accessoires -> Invite de commandes. Ensuite, on tape la commande :

```
ping <adresse_ip> -t
```

### 1. Connectivité Serveur / Utilisateur

Connectivité sur le switch	Port n°
Routeur	1
PC_ADMIN	41
PC_TEST	3

	Internet (172.16.1.1)	Switch (172.16.1.10)	PC_ADMIN	PC_TEST
PC_ADMIN	Non	Non	Oui	Non
PC_TEST	Non	Non	Non	Oui

## 2. Connectivité Serveur / Informatique

Connectivité sur le switch	Port n°
Routeur	1
PC_ADMIN	41
PC_TEST	17

	Internet (172.16.1.1)	Switch (172.16.1.10)	PC_ADMIN	PC_TEST
PC_ADMIN	Non	Non	Oui	Non
PC_TEST	Non	Non	Non	Oui

## 3. Connectivité Informatique / Utilisateur

Connectivité sur le switch	Port n°
Routeur	1
PC_ADMIN	17
PC_TEST	3

	Internet (172.16.1.1)	Switch (172.16.1.10)	PC_ADMIN	PC_TEST
PC_ADMIN	Oui	Oui	Oui	Non
PC_TEST	Non	Non	Non	Oui

## 4. Premières conclusions

Nos 3 VLANs sont bien isolés physiquement. Seul le VLAN n°1 (Informatique) permet d'administrer le Switch.

## VI. Configuration de l'architecture complète

### A. Vérifications

Afin de réaliser cette fois l'architecture complète du client, certains changements sont à appliquer. En effet, pour des raisons à la fois liées à la sécurité mais aussi à l'usage du VLAN n°1, nous allons fixer un port pour l'administration du Switch et cela exclut le VLAN Informatique de cette fonction avec cette architecture. Le Front Panel View (Monitor -> Views -> Front Panel View) est identique mais plus restrictif.

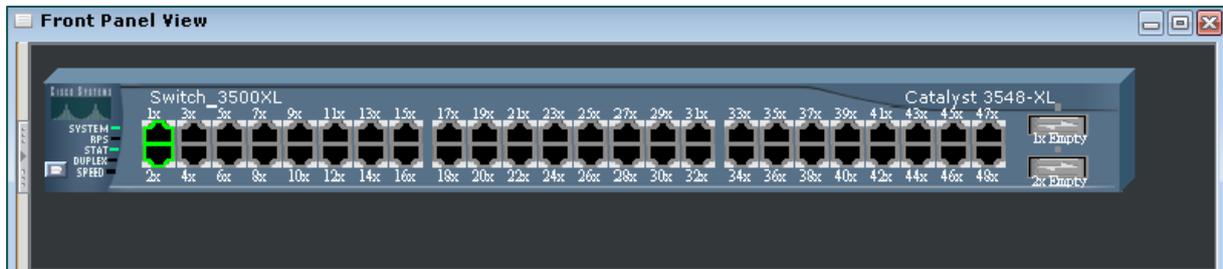


Figure 6- Front panel view, vérification de la connectique

### B. Création des VLANs

Nous devons créer cette fois un VLAN supplémentaire correspondant à l'accès à Internet.

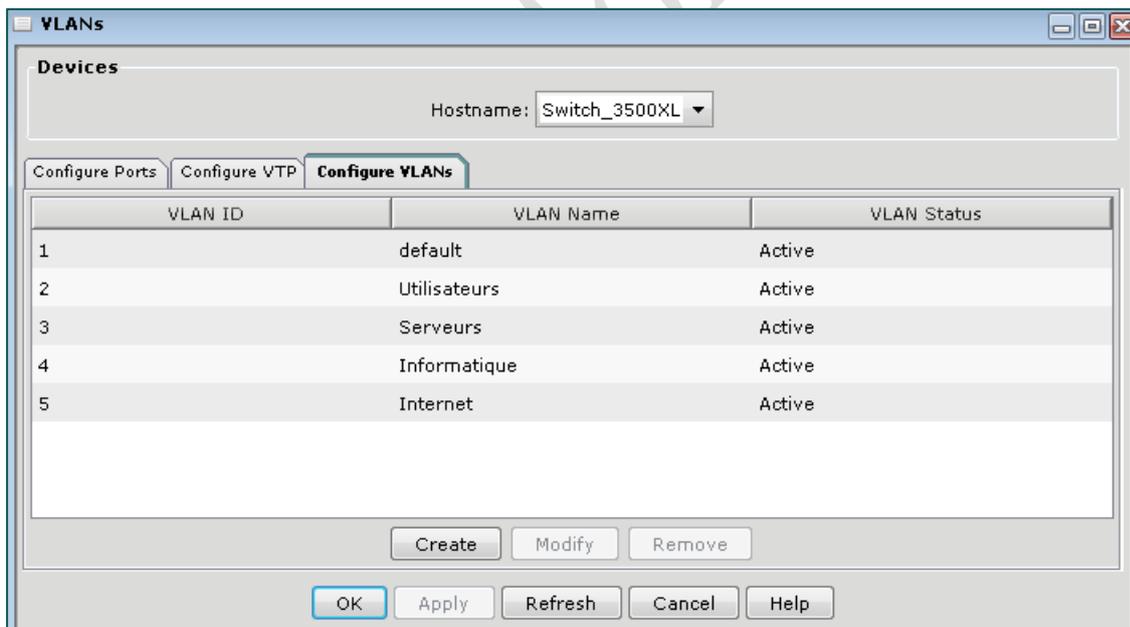


Figure 7 - Création de tous les VLANs

### C. Attribution des ports

La méthodologie d'affectation est similaire au chapitre précédent et ne nécessite pas d'information sur la méthodologie d'attribution. Cependant quelques précisions sont à fournir sur ces paramètres.

Le VLAN Internet doit être accessible depuis les autres VLANs il faut donc le rajouter dans tous les VLANs, il faut faire de même avec le VLAN Serveurs.

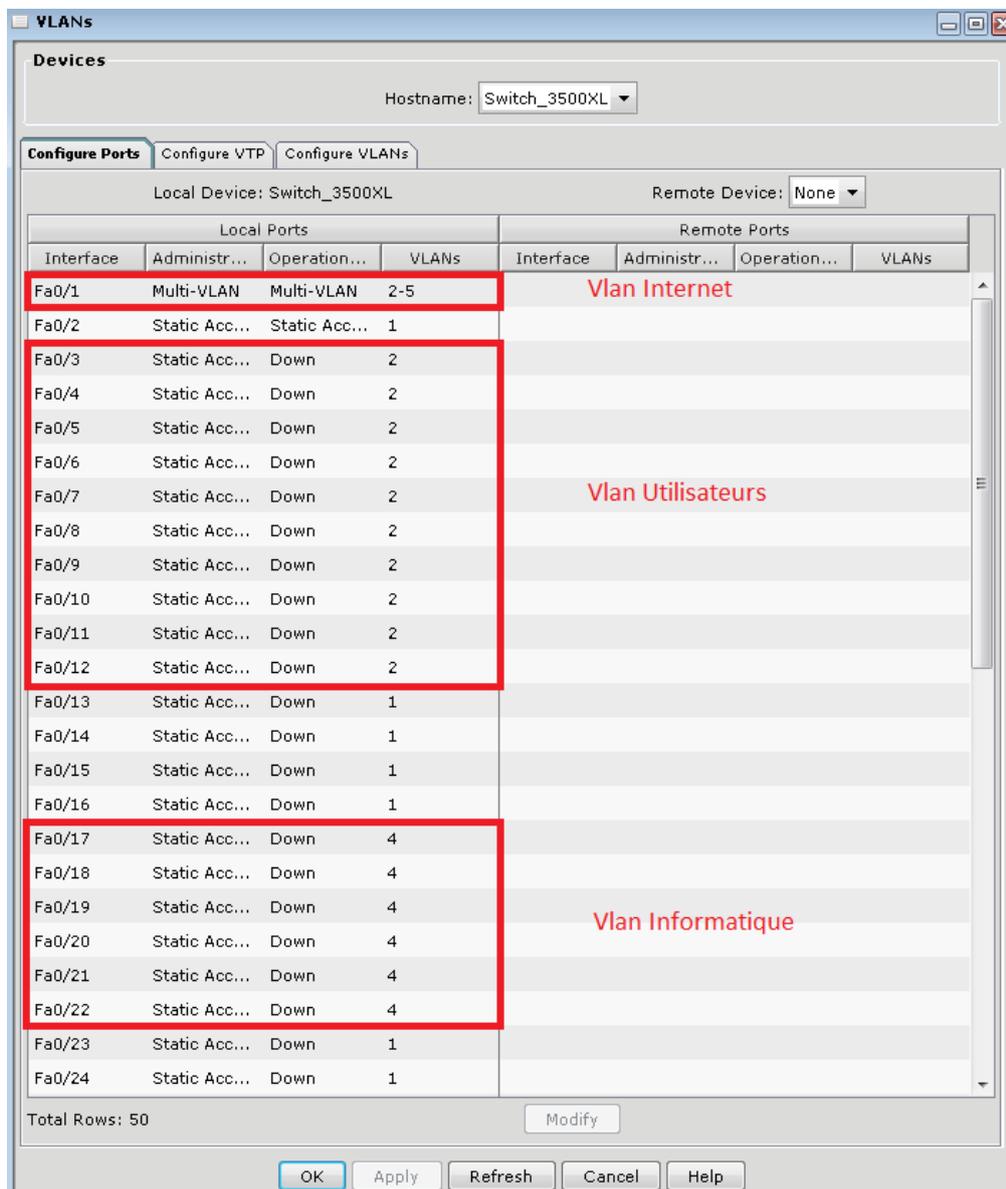


Figure 8 - Affectation des VLANs à chaque port (1 à 24)

**Astuce :** Pour assigner plusieurs VLANs à un port il suffit de choisir Multi-VLAN au lieu de Static Access.

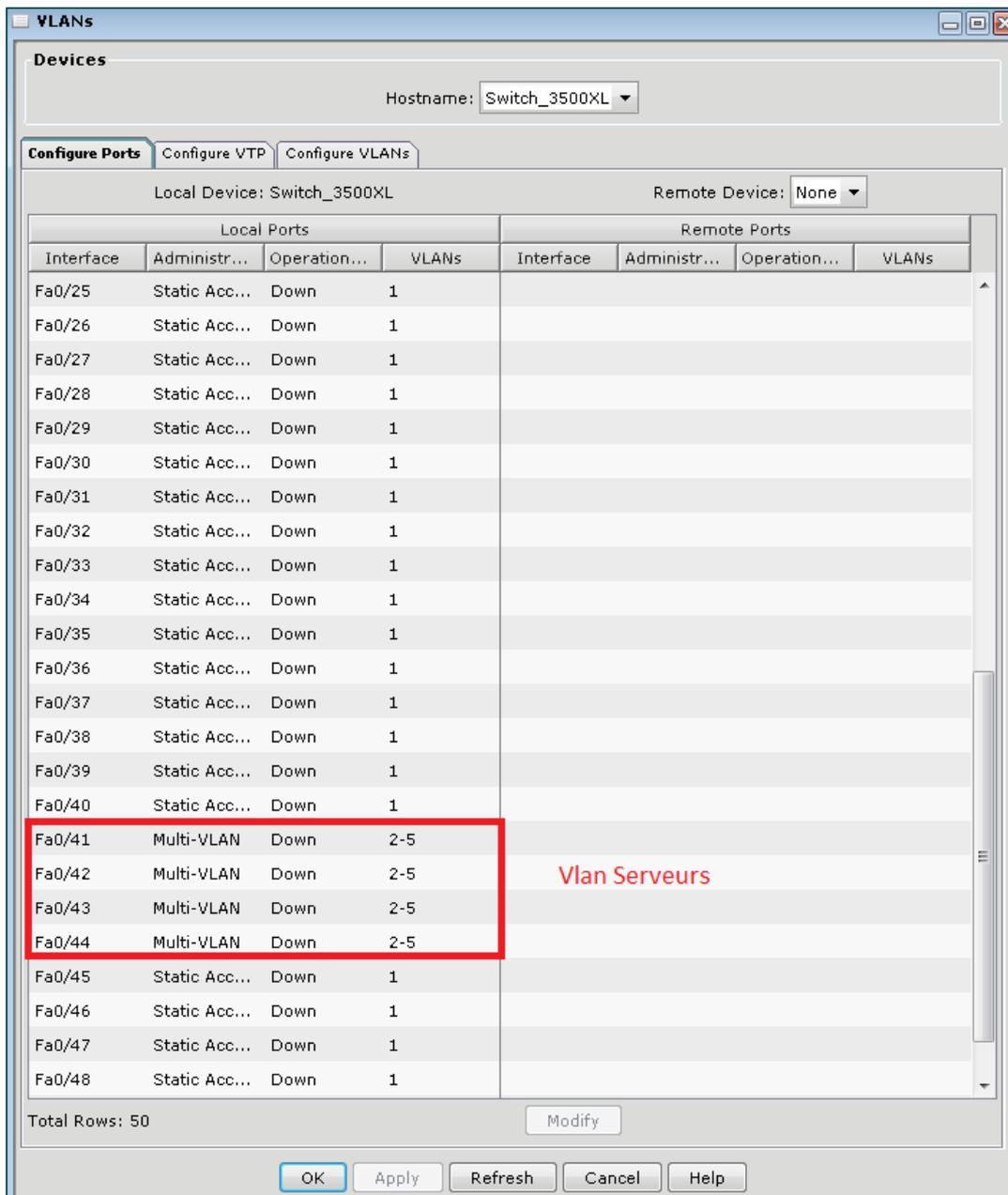


Figure 9- Affectation des VLANs à chaque port (25 à 48)

#### D. Tests de la configuration

La procédure de test est identique à la précédente la différence se situe simplement sur la communication inter-VLAN qui ne marche pas entre le pôle Informatique et le pôle Utilisateurs.

## VII. Configuration complète (CLI)

### A. Création des VLANs

Tout d'abord il faut se mettre en mode enable :

```
Switch_3500XL>en
Password:
Switch_3500XL#
```

Vous pouvez ensuite voir les VLANs déjà présents sur votre Switch en utilisant la commande **show vlan**, vous devez maintenant entrer la commande **vlan database** :

```
Switch_3500XL#vlan database
Switch_3500XL(vlan)#
```

**Attention** : Vous devez d'abord entrer dans « vlan database » afin de pouvoir créer un VLAN.

Ensuite faite la commande **vlan X** (X étant le VLAN ID) suivi de **name nom-de-vlan** :

```
Switch_3500XL(vlan)#vlan 2 name Utilisateurs

VLAN 2 added:
  Name: Utilisateurs
Switch_3500XL(vlan)#exit
APPLY completed.
Exiting....
```

**Attention** : Vous devez faire **exit** afin que les changements soient appliqués.

La commande **show vlan** devrait faire apparaître les changements.

### B. Attribution des ports

Pour affecter un port à un VLAN il faut utiliser les commandes suivantes dans l'ordre :

```
Switch_3500XL#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_3500XL(config)#interface fastethernet 0/3
```

*Permet d'accéder à l'interface de configuration du port 3*

```
Switch_3500XL(config-if)#switchport access vlan 2
```

*Affecte le port au VLAN 2*

```
Switch_3500XL(config-if)#exit
Switch_3500XL(config)#interface fastethernet 0/4
Switch_3500XL(config-if)#switchport access vlan 2
```

**Attention** : Répétez autant de fois qu'il le faut afin d'affecter tous les ports aux différents VLANs

La commande **write memory** permet de sauvegarder la configuration :

```
Switch_3500XL#write memory
Building configuration...
[OK]
```

Afin de configurer les ports en mode multi, pour les VLANs Internet et Serveurs, il faut suivre ces commandes :

```
Switch_3500XL#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_3500XL(config)#interface fastethernet 0/2
Switch_3500XL(config-if)#switchport mode multi vlan 2,3,4,5
```

*Permet d'assigner le port 2 aux VLANs 2, 3, 4 et 5.*

*Attention : Répétez la commande pour les ports du VLAN Serveurs (si la commande ne marche pas, séparer les numéros de VLANs par des espaces au lieu des virgules).*

Nolmë Informatique

## VIII. Annexes

### A. Glossaire

CLI : Command Line Interface. Interpréteur de commande.

DHCP : Dynamic Host Configuration Protocol. Protocole réseau permettant d'attribuer automatiquement une adresse IP.

DMZ : Sous-réseau informatique isolé.

DNS : Domain Name System. Système de correspondance entre adresse IP et nom.

FAI : Fournisseur d'Accès à Internet ou Provider.

LAN : Local Area Network. Réseau informatique local.

MTU : Taille maximale d'un paquet réseau pouvant être transmis en une fois.

VLAN : Virtual LAN. Réseau informatique logique indépendant.

VPN : Virtual Private Network. Réseau privé de communication sécurisé.

WAN : Wide Area Network. Réseau informatique couvrant une grande zone géographique.

WEP : Wired Equivalent Privacy. Mode de cryptage de communication pour les réseaux sans fil. Ce mode de sécurité est aujourd'hui obsolète du fait de sa faible robustesse face aux attaques.

WPA : Wi-Fi Protected Access. Mode de cryptage de communication pour les réseaux sans fil. Il tend aujourd'hui à être remplacé par le WPA2 plus sécurisé.

## B. Logiciels tiers

Au cours de ce document, il se peut que certains logiciels soient utilisés pour un point de vue technique ou simplement pour vérifier le fonctionnement d'un appareil. Ils sont présentés ici sommairement afin de comprendre leur utilité. Si toutefois vous désirez approfondir vos connaissances sur ces logiciels, nous vous invitons à visiter le site Internet de l'éditeur du logiciel en question.

Cisco – Network Assistant : GUI pour les Switches, routeurs et points d'accès Cisco

Cisco – ASDM : GUI pour la gamme ASA, PIX Cisco

Dependency Walker : Utilitaire Windows traçant les dépendances logicielles

Devolutions - Remote Desktop Manager : Logiciel de centralisation de connexions à distance

Filezilla : Client et serveur FTP pour Windows

NetSNMP : Outils de ligne de commande pour la supervision SNMP

NetStumbler 0.4.0 : Logiciel d'analyse de réseaux sans fil

Paessler - SNMP Tester : Logiciel d'analyse SNMP

Paessler - PRTG Network Monitor : Logiciel de supervision SNMP

PuTTY : Client Telnet / SSH pour Windows

Solarwinds - Kiwi SysLog Server : Serveur SYSLOG pour Windows (version gratuite ou payante)

WinPCap : Librairie de capture de trames réseaux pour Windows

Wireshark : Logiciel d'analyse de trames réseaux

## C. Autres annexes

Le site [www.cisco.com](http://www.cisco.com) est très riche en informations, n'hésitez pas à le consulter régulièrement.

