

vlan-management

MARK RODERICK

1. Les Fondamentaux : VLAN & Management

Qu'est-ce qu'un VLAN ?

Un **VLAN (Virtual Local Area Network)** est un regroupement logique d'équipements sur un même commutateur (switch), même s'ils ne sont pas physiquement sur le même segment. Cela permet d'isoler le trafic (ex: séparer la Compta de la Wi-Fi Invité).

Le VLAN de Management (Gestion)

C'est un VLAN **dédié uniquement à l'administration** des équipements réseaux (switches, routeurs, bornes Wi-Fi).

- **But** : Empêcher un utilisateur lambda d'accéder à l'interface de configuration du switch.
 - **Règle d'or** : Ne jamais utiliser le VLAN 1 (par défaut) pour le management. On crée souvent un VLAN spécifique (ex: VLAN 99).
-

2. Les Modes de Ports : Access vs Trunk

Pour qu'un VLAN circule, il faut configurer les ports du switch.

Mode	Description	Utilisation typique
Access	Le port appartient à un seul VLAN. Les données sortent "non-étiquetées" (untagged).	PC, Imprimantes, Serveurs.
Trunk	Le port laisse passer plusieurs VLANs en même temps en ajoutant une étiquette (Tag 802.1Q).	Entre deux switches ou vers un routeur.

3. Améliorer et Sauvegarder via Éditeur de Texte

Travailler sur un éditeur de texte (Notepad++, VS Code, Sublime Text) avant d'injecter la config est la meilleure pratique pour éviter les erreurs.

Comment améliorer sa config ?

1. **Nommage systématique** : Ne crée pas juste `vlan 10` , utilise `name VLAN_MARKETING` .
2. **Commentaires** : Utilise le symbole `!` (sur Cisco) pour expliquer pourquoi cette règle est là.
3. **Standardisation** : Crée un "template" (modèle) que tu réutilises sur tous tes switches.

Sauvegarder un Backup (Config de secours)

Il y a deux méthodes principales :

- **Méthode Manuelle (Copier/Coller)** :
 1. Dans ton terminal (Putty/TeraTerm), tape : `show running-config` .
 2. Sélectionne tout le texte affiché.
 3. Colle-le dans un fichier `.txt` ou `.cfg` sur ton PC.
 - **Méthode Automatisée (TFTP/SFTP)** :
 - Si tu as un serveur TFTP sur ton réseau :
 - `copy running-config tftp:`
 - Entre l'IP du serveur et le nom du fichier.
-

4. Déploiement : Comment "pousser" la config ?

Une fois que tu as préparé ton fichier texte proprement sur ton PC, voici comment le déployer :

Option A : Le copier-coller (Le plus simple)

1. Ouvre ton fichier texte.
2. Copie les lignes de commandes.
3. Va dans le mode configuration de ton switch (`conf t`).
4. Fais un clic droit (coller). Le switch exécute les lignes une par une.
5. **Important** : Tape `write memory` ou `copy run start` à la fin pour enregistrer de façon permanente.

Option B : Chargement via serveur (Le plus pro)

Si tu dois configurer 10 switches :

1. Place le fichier `config-switch-1.cfg` sur un serveur TFTP.
 2. Sur le switch, tape : `copy tftp://192.168.1.10/config-switch-1.cfg running-config` .
 3. Le switch fusionne sa config actuelle avec ton fichier.
-

Résumé pour une configuration "Pro" :

Checklist :

1. Créer les VLANs avec des noms clairs.
2. Assigner les ports (Access pour les PC, Trunk pour les liens inter-switches).
3. Configurer l'IP de management dans le VLAN dédié.
4. Tester la connectivité.
5. **Copier le texte dans un fichier de backup daté.**

Un comparatif des commandes pour les quatre constructeurs les plus courants. Vous remarquerez que **Cisco** et **Aruba (AOS-CX)** se ressemblent beaucoup, alors qu'**HP (ProCurve)** et **Fortinet** ont des logiques différentes.

1. Cisco (IOS / IOS-XE)

C'est la syntaxe de référence ("Port-Centric").

Action	Commande
Créer VLAN	<pre>vlan 10 name COMPTA</pre>
Port Access	<pre>interface Gi0/1 switchport mode access switchport access vlan 10</pre>
Port Trunk	<pre>interface Gi0/24 switchport mode trunk switchport trunk allowed vlan 10,20</pre>
Sauvegarder	<pre>write memory ou copy running-config startup-config</pre>

2. Aruba (AOS-CX) - Gammes 6000, 6100, 6300...

Aruba a modernisé son interface pour être très proche de Cisco.

Action	Commande
Créer VLAN	<pre>vlan 10 name COMPTA</pre>
Port Access	<pre>interface 1/1/1 vlan access 10</pre>
Port Trunk	<pre>interface 1/1/24 vlan trunk allowed 10,20 vlan trunk native 1</pre>
Sauvegarder	<pre>write memory</pre>

3. HP / Aruba (AOS-S) - Gammes 2530, 2930...

Ancienne syntaxe ProCurve. Ici, la logique est "VLAN-Centric" : on entre dans le VLAN pour dire quels ports y appartiennent.

Action	Commande
Créer VLAN	<pre>vlan 10 name COMPTA</pre>
Port Access	<pre>vlan 10 untagged 1 (Le port 1 est en accès dans le vlan 10)</pre>

Action	Commande
Port Trunk	<pre>vlan 10 tagged 24 (Le port 24 laisse passer le tag du vlan 10)</pre>
Sauvegarder	<pre>write memory</pre>

4. Fortinet (FortiSwitch CLI)

La logique Fortinet utilise des blocs `config / edit / set`.

Action	Commande
Créer VLAN	<pre>config switch vlan edit 10 set name COMPTA end</pre>
Port Access	<pre>config switch interface edit port1 set native-vlan 10 end</pre>
Port Trunk	<pre>config switch interface edit port24</pre>

Action	Commande
	<pre>set allowed-vlans 10 20 end</pre>
Sauvegarder	Automatique sur Fortinet (pas de <code>write mem</code> nécessaire).

Gestion des fichiers de configuration (Backup/Restore)

Pour tous ces switches, la méthode "Éditeur de texte" est la plus sûre :

Comment faire un Backup propre :

1. Affichez la configuration complète : `show running-config` (Cisco/Aruba) ou `show config` (HP).
2. Copiez le texte du terminal.
3. Collez-le dans **Notepad++** ou **VS Code**.
4. **Nettoyage** : Supprimez les lignes inutiles comme les certificats SSL ou les mots de passe hachés si vous voulez en faire un "Template".

Comment déployer (Restore) :

Si vous avez un switch neuf et que vous voulez injecter votre fichier texte :

1. Ouvrez votre fichier texte.
2. Connectez-vous en console au switch.
3. Passez en mode configuration (`conf t` ou `config`).
4. **Collez le texte par petits blocs** (environ 20-30 lignes à la fois) pour être sûr que le switch traite tout sans erreur de buffer.
5. Vérifiez avec un `show vlan` que tout est là.

Astuce de pro : Le "Reload in"

Sur Cisco et Aruba, avant de faire une modification risquée à distance sur un Trunk (ce qui pourrait vous couper l'accès), utilisez cette commande :

```
reload in 10
```

Cela dit au switch : "Si je ne confirme pas cette commande dans 10 minutes, redémarre tout seul pour reprendre l'ancienne config". C'est votre filet de sécurité !

Est-ce que tu as besoin d'un exemple de script complet pour un VLAN de Management spécifique ?

Small Business
cisco SG300-10 10-Port Gigabit Managed Switch
Language: English

Getting Started
Status and Statistics
Administration
Port Management
Smartport
VLAN Management
Default VLAN Settings
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
Private VLAN Settings
GVRP Settings
VLAN Groups
Voice VLAN
Access Port Multicast TV VLAN
Customer Port Multicast TV VLAN
Spanning Tree
MAC Address Tables
Multicast
IP Configuration
Security
Access Control
Quality of Service
SNMP

VLAN Settings

<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status	SNMP Traps
<input type="checkbox"/>	1		Default	Enabled	Enabled	
<input type="checkbox"/>	101	wifi	Static	Disabled	Enabled	
<input type="checkbox"/>	102	redondance	Static	Disabled	Enabled	
<input type="checkbox"/>	123	VWifi	Static	Disabled	Enabled	
<input type="checkbox"/>	127	VRedondance	Static	Disabled	Enabled	

Add... Edit... Delete

change en L3 pour acceder la routgae

Small Business
cisco SG300-10 10-Port Gigabit Managed Switch

- Getting Started
- ▶ Status and Statistics
- ▼ Administration
 - System Settings**
 - Console Settings
 - User Accounts
 - Idle Session Timeout
 - ▶ Time Settings
 - ▶ System Log
 - ▶ File Management
 - Reboot
 - Routing Resources
 - ▶ Diagnostics
 - Discovery - Bonjour
 - ▶ Discovery - LLDP
 - ▶ Discovery - CDP
 - Ping
 - Traceroute
- ▼ Port Management
 - Port Settings
 - Error Recovery Settings
 - Loopback Detection Settings
 - ▶ Link Aggregation
 - ▶ UDLD
 - ▶ Green Ethernet
- ▶ Smartport
- ▶ VLAN Management
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▶ Multicast
- ▶ IP Configuration
- ▶ Security
- ▶ Access Control

System Settings

System Settings

System Description: SG300-10 10-Port Gigabit Managed Switch

System Location: (0/160 characters used)

System Contact: (0/160 characters used)

Host Name: Use Default User Defined (0/58 characters used; Default: switchafeb)

System Mode: L2 L3

Custom Banner Settings

Login Banner:
(0/1000 characters used)

Welcome Banner:
(0/1000 characters used)



Small Business SG300-10 10-Port Gigabit Managed Switch

- Getting Started
- ▶ Status and Statistics
- ▼ Administration
 - System Settings
 - Console Settings
 - User Accounts
 - Idle Session Timeout
 - Time Settings
 - System Log
 - ▶ File Management
 - Reboot
 - Routing Resources
 - ▶ Diagnostics
 - Discovery - Bonjour
 - ▶ Discovery - LLDP
 - ▶ Discovery - CDP
 - Ping
 - Traceroute
 - ▶ Port Management
 - ▶ Smartport
 - ▼ **VLAN Management**
 - Default VLAN Settings
 - VLAN Settings
 - Interface Settings**
 - Port to VLAN
 - Port VLAN Membership
 - Private VLAN Settings
 - VRRP Settings

Interface Settings

Interface Settings Table

Filter: *Interface Type* equals to

	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Primary VLAN	Secondary
<input type="radio"/>	1	GE1	Trunk	1	Admit All	Enabled		
<input type="radio"/>	2	GE2	Trunk	1	Admit All	Enabled		
<input type="radio"/>	3	GE3	Trunk	101	Admit All	Enabled		
<input type="radio"/>	4	GE4	Trunk	102	Admit All	Enabled		
<input type="radio"/>	5	GE5	Trunk	123	Admit All	Enabled		
<input type="radio"/>	6	GE6	Trunk	127	Admit All	Enabled		
<input type="radio"/>	7	GE7	Trunk	1	Admit All	Enabled		
<input type="radio"/>	8	GE8	Trunk	1	Admit All	Enabled		
<input type="radio"/>	9	GE9	Trunk	1	Admit All	Enabled		
<input type="radio"/>	10	GE10	Trunk	1	Admit All	Enabled		