

Switch Alcatel-Lucent OS6350

Testé sur OS6350-P avec AOS 6.7.2.107R01

- [Connexion au Switch](#)
- [Commandes de base](#)
- [Mettre à jour l'AOS](#)
- [Supprimer la configuration](#)
- [Supprimer le mot de passe admin](#)
- [Configuration des VLAN](#)
- [Configuration VLAN voix, LLDP et QOS voix](#)
- [Configuration de Telnet, SSH et WEB](#)
- [Configuration de l'agrégation de liens](#)
- [Configuration du NTP](#)
- [Configuration de Syslog](#)
- [Configuration des ports](#)
- [Configuration de Port-security](#)
- [Configuration du STP](#)
- [Configuration du DHCP](#)
- [Configuration de la bannière](#)
- [Configuration du 802.1X](#)
- [Configuration du SNMP](#)
- [Etats des ports](#)
- [Importer et Exporter la configuration via TFTP](#)
- [Gestion de la table ARP](#)

Connexion au Switch

Pour vous connecter au switch en port console, il vous faut l'adaptateur Alcatel :

alcatel-serie.jpg

- Bits : 9600
- Data bits : 8
- Parity : none
- Stop bits : 1
- Flow control : none

Commandes de base

Sauvegarder la configuration

Les switchs Alcatel fonctionnent avec deux configurations, la working et la certified

Quand le switch démarre, si les deux configurations sont identiques, le switch démarre sur la working

Si les deux configurations ne sont pas identique, le switch démarre sur la certified. Cependant, il n'est pas possible de modifier la configuration en mode certified.

Pour sauvegarder la configuration

```
-> copy running-config working
```

puis

```
-> copy working certified
```

Ou en une fois

```
-> write memory flash-synchro
```

Pour voir sur quel configuration le switch à démarrer

```
-> show running-directory
```

CONFIGURATION STATUS

```
Running CMM          : PRIMARY,  
CMM Mode             : MONO CMM,  
Current CMM Slot     : 1,  
Running configuration : WORKING,  
Certify/Restore Status : CERTIFIED
```

SYNCHRONIZATION STATUS

```
Running Configuration : SYNCHRONIZED,
```

Afficher la configuration

```
-> show configuration snapshot
```

Redémarrer

```
-> reload
```

Hostname, Contact et Localisation

```
-> system name <name>  
-> system contact <contact>  
-> system location <localisation>
```

DNS

```
-> ip name-server 194.2.0.20 194.2.0.50  
-> ip domain-lookup  
-> no ip domain-lookup
```

Vérification

```
-> show dns
```

Route par défaut

```
-> ip static-route 0.0.0.0/0 gateway 192.168.1.1 metric 1
```

Création d'un utilisateur

```
-> user <name> password <password> read-write all
```

Afficher les informations

```
-> show microcode  
-> show hardware info  
-> show chassis  
-> show module  
-> show fan  
-> show temperature
```

Afficher les utilisateurs connectés

```
-> who
```

Afficher la table MAC

```
-> show mac-address-table
```

Changer le prompt

```
-> session prompt default "switch -> "
```

Désactivation du cloud-agent

```
-> cloud-agent admin-state disable
```

Changement de prompt

```
-> session prompt default <NOM>
```

```
-> write memory flash-synchro
```

Mettre à jour l'AOS

Etape 0 : Vérification de la version

```
-> show microcode
```

Package	Release	Size	Description
-----+-----+-----+-----			
KF3base.img	6.7.2.52.R01	15425911	Alcatel-Lucent Base Software
KF3os.img	6.7.2.52.R01	3693582	Alcatel-Lucent OS
KF3eni.img	6.7.2.52.R01	6533416	Alcatel-Lucent NI software
KF3secu.img	6.7.2.52.R01	602269	Alcatel-Lucent Security Management

Etape 1 : Donner une adresse IP au switch

```
-> ip interface "vlan1" address 192.168.1.10 mask 255.255.255.0 vlan 1
```

Etape 2 : Accorder les droits de connexion au serveur ftp du switch

```
-> aaa authentication ftp local
```

```
-> session timeout ftp 60
```

Etape 3 : Copier les nouveaux fichiers dans le répertoire working

À l'aide d'un client FTP, copiez les nouveaux fichiers dans le répertoire working.

Etape 4 : Copier le contenu du dossier working dans le dossier certified

```
-> copy working certified
```

```
SUN DEC 31 00:08:20 : CSM-CHASSIS (103) info message:
```

```
+++ == CSM == CERTIFYing software process started
```

```
+++ == CSM == Setting CERTIFY Timeout for 800 seconds
```

```
from /flash/working to /flash/certified
```

```
Copying KF3base.img ..... completed
```

```
from /flash/working to /flash/certified
```

```
Copying KF3eni.img ..... completed
```

```
from /flash/working to /flash/certified
```

```

Copying KF3fpga.upgrade_kit ..... completed
from /flash/working to /flash/certified
Copying kf3miniboot.bs ..... completed
from /flash/working to /flash/certified
Copying KF3os.img ..... completed
from /flash/working to /flash/certified
Copying KF3secu.img ..... completed
from /flash/working to /flash/certified
Copying kf3u-boot.bin ..... completed
from /flash/working to /flash/certified
Copying software.lsm ..... completed

```

```
+++ == CSM == Stack 1 Certify process Completed
```

```
SUN DEC 31 00:09:03 : CSM-CHASSIS (103) info message:
```

```
+++ == CSM == CERTIFY process completed successfully
```

Si vous obtenez l'erreur suivante : **ERROR: Invalid request, CERTIFY requested while running on certified**

Il faut redémarrer le switch en mode working avec la commande suivante :

```
-> reload working no rollback-timeout
```

Etape 5 : Reboot

```
-> reload
```

```
Confirm Reload (Y/N) : y
```

Etape 6 : Vérification de la version

```
-> show microcode
```

Package	Release	Size	Description
KF3base.img	6.7.2.107.R01	15601299	Alcatel-Lucent Base Software
KF3os.img	6.7.2.107.R01	3693727	Alcatel-Lucent OS
KF3eni.img	6.7.2.107.R01	6575742	Alcatel-Lucent NI software
KF3secu.img	6.7.2.107.R01	618461	Alcatel-Lucent Security Management

Supprimer la configuration

Pour supprimer la configuration, il faut utiliser ces deux commandes :

```
-> rm /flash/working/boot.cfg  
-> rm /flash/certified/boot.cfg  
-> reload working no rollback-timeout
```

Les deux premières commandes vont supprimer la configuration courante, et la configuration de secours.

Puis nous redémarrons le switch sur la partition working

Supprimer le mot de passe admin

Pour remettre le mot de passe par défaut d'un switch alcatel, il faut entrer en mode miniboot.

Pour cela, dès le début du démarrage du switch, appuyer sur "S" pour entrer en mode miniboot.

Interrupt boot sequence by pressing "s"

Une fois dans le miniboot, entrez : cd "network" pour aller dans le répertoire "network"

```
[Miniboot]->cd "network"  
value = 0 = 0x0
```

puis listez les fichiers avec "ls"

```
[Miniboot]->ls  
.  
..  
userTable6  
lockoutSetting  
policy.cfg  
ipTable  
accessTable  
ssh_host_dsa_key  
ssh_host_dsa_key.pub  
ssh_host_rsa_key  
ssh_host_rsa_key.pub  
userPrivPasswordTable  
value = 0 = 0x0
```

pour supprimer la liste des utilisateurs, il faut supprimer le fichier "userTable"

```
[Miniboot]->xdelete "userTable6"  
value = 0 = 0x0
```

puis rebooter le switch

```
[Miniboot]->reboot
```

```
WARNING: "sysResetHardwareFlag" flag is SET, forcing CMM board reset.
```

Le mot de passe admin est maintenant celui par défaut :

login : admin / password : switch

Configuration des VLAN

Virtual Local Area Network

Créer un VLAN

-> vlan 100 enable

Nommer un VLAN

-> vlan 100 name voix

Supprimer un VLAN

-> no vlan 100

Activer ou Désactiver un VLAN

-> vlan 100 enable

-> vlan 100 disable

Ajouter un port à un VLAN non tagué

-> vlan 100 port default 1/1

Supprimer un port d'un VLAN non tagué

-> vlan 100 no port default 1/1

Ajouter un port à un VLAN tagué

-> vlan 100 802.1q 1/1

Supprimer un port d'un VLAN tagué

-> vlan 100 no 802.1q 1/1

Afficher les informations des VLANs

```
-> show vlan
-> show vlan 100
-> show vlan port
-> show vlan 100 port
-> show vlan port 1/1
```

Assigner une adresse IP à un VLAN

```
-> ip interface "vlan100" address 192.168.1.100 mask 255.255.255.0 vlan 100
```

options :

```
-> ip interface dhcp-client vlan 100
-> ip interface dhcp-client admin enable
-> ip interface dhcp-client release
-> ip interface dhcp-client renew
```

Supprimer une adresse IP à un VLAN

```
-> no ip interface <nom_interface>
```

Configurer un port en mode Trunk

```
-> vlan 100 802.1q 1/24
-> vlan 101 802.1q 1/24
```

A faire autant de fois qu'il y a de vlan a faire passer dans le Trunk

Configurer un port en mode Mixte

```
-> vlan 101 port default 1/1
-> vlan 100 802.1q 1/1
```

Port 1/1 en access data et tag voix

Configuration VLAN voix, LLDP et QOS voix

Configuration

Configuration d'un port mixte (vlan voix taggué + vlan data non taggué)

```
-> vlan 101 port default 1/1  
-> vlan 100 802.1q 1/1
```

Configuration du LLDP

Link Layer Discovery Protocol

```
-> lldp network-policy 1 application voice vlan 100 l2-priority 5 dscp 46  
-> lldp chassis tlv med capability enable network-policy enable  
-> lldp chassis med network-policy 1
```

Configuration de la QOS voix

Quality of Service

```
-> qos enable  
-> policy condition IPphoneDSCP DSCP 46  
-> policy action IPphone-act priority 5  
-> policy rule IPphone-rule condition IPphoneDSCP action IPphone-act  
-> qos apply
```

Configuration de Telnet, SSH et WEB

Configuration de SSH

Secure Shell

```
-> ip service ssh  
-> aaa authentication ssh local  
-> session timeout cli 30  
-> session login-attempt 5
```

Vérification

```
-> show ssh config  
SSH = Enabled  
SCP/SFTP = Enabled  
Public Key Authentication Enforced = False  
TCP-Port Number = 22
```

Configuration de TELNET

Terminal network

```
-> aaa authentication telnet local
```

Configuration WEB

World Wide Web

En HTTP

```
-> aaa authentication http local  
-> http server
```

En HTTPS

-> https server

-> https ssl

Configuration de l'agrégation de liens

LACP

```
-> lacp linkagg 1 size 2
-> lacp linkagg 1 name "LACP1"
-> lacp linkagg 1 admin state enable
-> lacp linkagg 1 actor admin key 1
-> lacp agg 1/12 actor admin key 1
-> lacp agg 1/13 actor admin key 1
-> vlan 100 802.1q 1
-> vlan 101 802.1q 1
-> vlan 102 802.1q 1
```

Vérification

```
-> show linkagg
-> show linkagg agg 1
-> show linkagg port
```

STATIC

```
-> static linkagg 2 size 2
-> static agg 1/14 agg num 2
-> static agg 1/15 agg num 2
```

Configuration du NTP

Network Time Protocol

Introduction

Pour effectuer une synchronisation NTP, il faut tout d'abord que le switch puisse aller sur internet

```
-> ip interface "vlan1" address 192.168.10.100 mask 255.255.255.0 vlan 1 ifindex 1
-> ip static-route 0.0.0.0/0 gateway 192.168.10.1 metric 1
```

Passons à la configuration du NTP

```
-> ntp server 194.2.0.28 prefer
-> ntp server 38.229.59.9
-> ntp server enable
-> ntp server synchronised
```

Configuration de la timezone

```
-> system timezone CET
-> system daylight savings time start last sunday in march at 02:00 end last sunday in october at 03:00
-> system daylight savings time enable
```

ou

```
-> system timezone +01:00
-> system daylight savings time start last sunday in march at 02:00 end last sunday in october at 03:00
-> system daylight savings time enable
```

Vérification

```
-> show ntp server status
IP address      = 38.229.59.9,
Host mode       = client,
Peer mode       = server,
Prefer          = yes,
```

Version = 4,
Key = 0,
Stratum = 2,
Minpoll = 6 (64 seconds),
Maxpoll = 10 (1024 seconds),
Delay = 0.167 seconds,
Offset = 660733522.277 seconds,
Dispersion = 0.953 seconds
Root distance = 0.083,
Precision = -20,
Reference IP = 172.16.21.35,
Status = configured : reachable : rejected,
Uptime count = 1402 seconds,
Reachability = f,
Unreachable count = 0,
Stats reset count = 1043 seconds,
Packets sent = 6,
Packets received = 4,
Duplicate packets = 0,
Bogus origin = 0,
Bad authentication = 0,
Bad dispersion = 0,
Last Event = peer changed to reachable,

IP address = 194.2.0.28,
Host mode = client,
Peer mode = server,
Prefer = no,
Version = 4,
Key = 0,
Stratum = 2,
Minpoll = 6 (64 seconds),
Maxpoll = 10 (1024 seconds),
Delay = 0.017 seconds,
Offset = 660733522.272 seconds,
Dispersion = 1.952 seconds
Root distance = 0.000,
Precision = -23,
Reference IP = 172.19.123.3,

```
Status          = configured : reachable : rejected,  
Uptime count    = 1402 seconds,  
Reachability    = 7,  
Unreachable count = 0,  
Stats reset count = 1261 seconds,  
Packets sent    = 3,  
Packets received = 3,  
Duplicate packets = 0,  
Bogus origin    = 0,  
Bad authentication = 0,  
Bad dispersion  = 0,  
Last Event      = peer changed to reachable,
```

et

```
-> show ntp client  
Current time:      Wed, Dec 8 2021  9:47:58.667 (UTC),  
Last NTP update:   Wed, Dec 8 2021  9:47:28.033 (UTC),  
Server reference:  38.229.59.9,  
Client mode:       enabled,  
Broadcast client mode: disabled,  
Broadcast delay (microseconds): 4000,  
Server qualification: synchronized
```

Il est aussi possible de régler l'heure et la date à la main

```
-> system date 08/12/2021  
-> system time 10:48:00
```

Supprimer un serveur NTP :

```
-> no ntp server 194.2.0.28 prefer
```

Configuration de Syslog

Transmission de journaux

Activation de Syslog

```
-> swlog
```

Stocker les logs dans la mémoire flash

```
-> swlog output flash
```

Envois des logs sur un serveur Syslog

```
-> swlog output socket 192.168.1.100
```

```
-> swlog output console
```

Afficher les logs

```
-> show swlog
```

Effacer les logs

```
-> swlog clear
```

Afficher les logs d'une heure précise

```
-> show log swlog timestamp <mois/jour/année> <heure:minute>
```

Configuration des ports

Introduction

Nous allons voir comment configurer les ports de notre switch

Vitesse

```
-> interface 1/1 autoneg disable  
-> interface 1/1 speed 10  
-> interface 1/1 speed 100  
-> interface 1/1 speed 1000
```

Duplex

```
-> interface 1/1 duplex full  
-> interface 1/1 duplex half
```

Description

```
-> interfaces 1/1 alias <nom>
```

POE

```
-> lanpower start 1  
-> lanpower stop 1
```

Port mirroring

Pour configurer le port mirroring

```
-> port mirroring 1 source 1/1 destination 1/24 enable
```

Pour désactiver le port mirroring

```
-> no port mirroring 1
```

Pour voir le statut

-> show port mirroring status

Configuration de Port-security

Activation de port-security

```
-> port-security 1/1 admin-status enable
```

Limite d'adresse MAC

```
-> port-security 1/1 maximum 4
```

Violation de port

Il existe 3 modes :

- **Restrict:** Bloque le trafic non autorisé, mais autorise le reste
- **Discard:** Les adresses MAC apprises sont oubliées, aucun trafic n'est autorisé, mais le port reste UP
- **Shutdown:** Les adresses MAC apprises sont oubliées, aucun trafic n'est autorisé, le port devient DOWN

```
-> port-security 1/1 violation restrict  
-> port-security 1/1 violation discard  
-> port-security 1/1 violation shutdown
```

Ajouter une adresse MAC manuellement

```
-> port-security 1/2 mac 00:00:00:00:00:12
```


Configuration du STP

Configuration générale

```
-> bridge mode flat
```

puis choisir un protocole :

```
-> bridge protocol mstp  
-> bridge protocol rstp  
-> bridge protocol stp  
-> bridge protocol 1W  
-> bridge protocol 1D
```

1. MSTP : Création de plusieurs instances STP
2. RSTP : Convergence plus rapide que le STP
3. STP : Le classique

Configuration 1x1

```
-> bridge mode 1x1  
-> bridge 1x1 10 priority 4096
```

Configuration du DHCP

Etape 1 : Connexion au serveur FTP du switch

```
-> ip interface "vlan1" address 192.168.1.1 mask 255.255.255.0 vlan 1
-> aaa authentication ftp local
-> session timeout ftp 60
```

Etape 2 : Création des fichiers de configuration

Sur votre ordinateur, créer un fichier : dhcpd.pcy

```
PingDelay = 200
PingAttempts = 3
PingSendDelay = 1000
DefaultLease = 86400
```

Créer un autre fichier : dhcpd.conf

```
subnet 192.168.1.0 netmask 255.255.255.0
{
dynamic-dhcp range 192.168.1.50 192.168.100.100
{
option subnet-mask 255.255.255.0;
option routers 192.168.1.1;
option domain-name-servers 192.168.1.1;
option domain-name-servers 192.168.1.200;
option domain-name "lan.local";
option dhcp-lease-time 30000;
}
}
```

Le fichier dhcpd.conf stock la configuration du serveur DHCP

Etape 3 : Envoyer les fichiers sur le switch

Via un client FTP, envoyer les deux fichiers dans le répertoire /flash/switch

Etape 4 : Démarrer le serveur DHCP

```
-> dhcp-server restart
```

```
MON JAN 01 02:22:02 : DHCP-SERVER (140) info message:  
+++ /flash/switch/dhcpd.conf processed with 1 subnets
```

```
-> dhcp-server enable
```

```
MON JAN 01 02:22:05 : DHCP-SERVER (140) info message:  
+++ dhcp-server Enabled
```

Autre :

Désactiver le serveur DHCP :

```
-> dhcp-server disable
```

```
MON JAN 01 02:22:05 : DHCP-SERVER (140) info message:  
+++ dhcp-server Disabled
```

Supprimer les deux fichiers : dhcpd.pcy et dhcpd.conf

DHCP Snooping

Activation :

```
-> ip helper dhcp-snooping enable
```

Configuration des ports

```
-> ip helper dhcp-snooping port 1/1 trust  
-> ip helper dhcp-snooping port 1/1 block  
-> ip helper dhcp-snooping port 1/1 client-only
```

Trust : Autorise les requêtes dhcp

Block : Bloque les requêtes dhcp

Client-only : Autorise les requêtes depuis le port

Activation sur un VLAN

```
-> ip helper dhcp-snooping vlan 10 <enable | disable>
```

Vérification de l'adresse MAC

```
-> ip helper dhcp-snooping mac-address verification <enable | disable>
```

Vérifications

```
-> show ip helper dhcp-snooping vlan  
-> show ip helper dhcp-snooping port
```

Relai DHCP

Activation :

```
-> ip helper address 192.168.1.20
```

Activation sur un VLAN :

```
-> ip helper address 192.168.1.20 <VLAN_ID>
```

Configuration de la bannière

Activer la bannière

```
-> session banner cli <nom_fichier.txt>
```

Désactivation de la bannière

```
-> session banner no cli
```

Configuration

Ajouter une adresse ip au switch et activer le FTP

```
-> ip interface "vlan1" address 192.168.1.10 mask 255.255.255.0 vlan 1
-> aaa authentication ftp local
-> session timeout ftp 60
```

Via un client FTP, connectez-vous au switch et allez dans /flash/switch

Editer le fichier : pre_banner.txt

```
*****
* This access is restricted to authorised personnel *
* Unauthorized Access Prohibited!                  *
*****
```

Enregistrer.

os6350-banniere.png

Configuration du 802.1X

Le 802.1X permet l'authentification des utilisateurs sur le réseau.

Configuration

```
-> aaa radius-server serveur2 host 192.168.1.100 auth-port 1812 acct-port 1813 key "P@ssw0rd"  
-> aaa authentication 802.1x serveur2
```

Configuration des ports

```
-> vlan port mobile 1/1  
-> vlan port 1/1 802.1x enable
```

Si l'authentification est réussie, le port est placé dans le VLAN 101, sinon dans le VLAN 666.

```
-> 802.1x 1/1 supplicant policy authentication pass vlan 101 fail vlan 666
```

Vérifications

```
-> show 802.1x 1/1  
-> show 802.1x users
```

Configuration du SNMP

Configuration utilisateur

```
-> aaa authentication snmp local
-> user snmpuser password P@ssword read-only all no auth
```

Configuration SNMP

```
-> snmp security no security
-> snmp community map mode enable
-> snmp community map "public" user "snmpuser" on
-> snmp station @ip "snmpuser" v2 enable
```

Vérifications

```
-> show snmp station
```

ipAddress/udpPort	status	protocol	user
192.168.1.200/162	enable	v2	Admin

et

```
-> show snmp community map
```

Community mode : enabled

status	community string	user name
enabled	snmpmaptest	Admin

Etats des ports

Introduction

Voici l'état des voyant des switchs Alcatel

Explications

Désactivé	Aucun lien ou port shut
Vert	UP 1000Mbps
Orange	UP 1000Mbps avec POE

Importer et Exporter la configuration via TFTP

Exporter la configuration vers un serveur TFTP

```
-> tftp 192.168.3.55 put source-file /flash/working/boot.cfg destination-file config_sw.txt
```

Importer la configuration depuis un serveur TFTP

```
tftp 192.168.3.55 get source-file config_sw.txt destination-file /flash/working/boot.cfg
```

Gestion de la table ARP

ARP : Address Resolution Protocol

Voir la table ARP du switch

```
-> show arp
```

Ajouter / supprimer un équipement dans la table ARP

```
-> arp <ip> <mac-address>
```

```
-> no arp <ip>
```

Effacer la table ARP

```
-> clear arp-table
```