ALCATEL

COMMANDES DE BASE

Compte par défaut : admin / switch

Remettre en configuration usine

```
dir
delete *.log                    nettoyer la racine
delete *.err                    l'étoile sélectionne tous les fichiers dont l'extension suit
cd working
delete boot.cfg
cd ..
cd certified
delete boot.cfg
cd ..
cd network
delete userTable
delete qos.cfg                                  si QOS utilisée
delete policy.cfg                               si règles mises en place
reload working no rollback-timeout
```

Mise à jour du switch par ftp

```
show microcode                                  version des fichiers installés
```

effacer les fichiers images (*.img) dans le répertoire /flash/working

```
cd working
dir
del *.img
```

envoyer les nouveaux fichiers images (*.img) dans le répertoire /flash/working

```
ftp @IP_hôte
cd nom_dossier                                  sélection du répertoire sur le serveur
dir                                             liste un dossier
get nom                                         télécharge un fichier depuis le serveur
put nom                                         envoie un fichier
pwd                                             affiche le répertoire courant
delete nom                                      supprime un fichier
quit                                            ferme la session FTP
```

installer les nouveaux fichiers

cd working
install *.img

Paramétrer le switch : nom / heure / date …

system name nom_switch — nomme le switch
session prompt default nom_switch — nomme le CLI
session timeout cli sec — délai avant déconnexion automatique
system location lieu
system contact contact
system date mm/jj/yyyy
system time hh:mm:ss
session banner cli /flash/nom_banner.txt

Manipuler les fichiers

mkdir nom_dossier
rename ancien_nom nvo_nom
delete nom_fichier

Redémarrage

reload working no rollback-timeout — charge la working dans la running sans délai
reload working rollback-timeout sec
charge la working dans la running avec un délai spécifié en sec, permet de récupérer une configuration fonctionnelle précédente si la configuration en cours n'est plus valide
reload — redémarrage immédiat
reload at hh:mm
reload in mm ou hh:mm — compte à rebours

Sauvegarde

write memory	enregistre la configuration dans la working
copy running-config working	si running-directory ≠ working
copy working certified	enregistre la configuration dans la certified

Commandes d'affichages

show running-directory	affiche les répertoires de sauvegarde utilisés
write terminal	affiche la configuration courante

ACCES et AUTHENTIFICATION

Active / Désactive les types d'accès

aaa authentication default local	accès par défaut	
aaa authentication console local	accès console	
no aaa authentication telnet	accès TELNET	port 23
no aaa authentication http	accès WEB	port 80
aaa authentication snmp local	accès SNMP	port 162
no aaa authentication ftp	accès FTP	port 21
aaa authentication ssh local	accès SecureSHell	port 22

Commandes d'affichages

show aaa authentication	affiche les accès activés ou non

Créer un utilisateur

Il existe 3 utilisateurs par défaut : admin, default et public

user nom_user password password	l'utilisateur créé prend les droits par default
user nom_user MD5/SHA password password	mdp avec hashage MD5 ou SHA
user nom_user MD5+DES/SHA+DES password password	
mdp avec hashage MD5 ou SHA et encryption du flux en DES (notion de privacy)	
user nom_user read-only all/none	donne les droits de lecture à l'utilisateur
user nom_user read-write all/none	donne tous les droits à l'utilisateur
user password-size min 14	force le mot de passe à 14 caractères min

exemple

user nom_user read-only all read-write none MD5 password password
user nom_user read-only none read-write all SHA+DES password password

Effacer un utilisateur

no user nom_user

Commandes d'affichages

show user	affiche les utilisateurs

CONFIGURATION DES INTERFACES

interfaces slot/port — pour sélectionner une interface
interfaces slot/port_début-port_fin — pour sélectionner plusieurs interfaces
interfaces slot — pour sélectionner une carte

interfaces slot/port alias description — nomme l'interface
interfaces slot/port speed 10/100/1000/auto — défini la vitesse
interfaces slot/port duplex full/half/auto
défini la méthode de transmission des données
interfaces slot/port crossover MDI/MDIX/auto
défini le croisement des données sur l'int ; MDI pour HUB et SW / MDIX pour stations
interfaces slot/port autoneg enable/disable
autonégociation de la vitesse, du duplex et du MDIX
interfaces slot/port max frame size — défini la taille de la trame (MTU)

interfaces slot/port admin up/down — active / désactive une interface

Commandes d'affichages

show interfaces — affiche le détail des interfaces
show interfaces port — affiche l'état des interfaces et leurs alias
show interfaces status
affiche l'état des interfaces, l'autonégociation, la vitesse, le duplex
show interfaces capability
affiche l'état et les valeurs possibles de l'autonégociation, la vitesse, le duplex, le crossover

Configurer la sécurité

port-security slot/port enable/disable — active/désactive la sécurité

port-security slot/port maximum nbr_@MAC_apprises_du_port
port-security slot/port violation shutdown/restrict — action entreprise si intrusion
shutdown = éteint le ! / restrict = empêche le traffic pour les @MAC non autorisées
port-security slot/port shutdown sec — tps d'apprentissage de l'@MAC

port-security slot/port mac-range low @MAC high @MAC — plage @MAC
port-security slot/port mac-range — remet par défaut
port-security slot/port mac @MAC — ajout manuel @MAC
port-security slot/port no mac @MAC — supprime une @MAC
port-security slot/port release — efface les @MAC apprises par le !

Mirroring

port mirroring num_session source slot/port destination slot/port enable/disable
active/désactive un mirrorring d'un port vers un autre

no port mirroring num_session supprime le mirroring

PARAMETRAGE MAC

Table d'adresses MAC

mac-address-table permanent/learned @MAC slot/port ajouter une @MAC manuellement

mac-address-table aging-time tps_sec
tps de validité de l'@MAC en secondes

Commandes d'affichages

show mac-address-table affiche la table d'@MAC
show mac-address-table count
affiche le nombre d'@MAC apprises manuellement / dynamiquement
show mac-address-table aging-time affiche le tps de validité des @MAC par VLAN
show arp affiche la table de relation entre @MAC et @IP

ARP

Table ARP

arp @IP @MAC alias arp-name nom_entrée
ajoute une entrée dans la table ARP / l'option alias => switch agit comme un proxy, il ne donne que son @MAC et non celle de l'interface
clear arp-cache vide la table ARP

Commandes d'affichages

show arp affiche la table de relation entre @MAC et @IP

PARAMETRAGE IP

Configuration IP

ip interface name address @IP mask @mask admin enable/disable vlan id forward/no forward
routable ou non local-proxy-arp/no local-proxy-arp même @MAC pour tous les ports du VLAN
eth2/snap type d'encapsultion primary/no primary car plusieurs @IP possibles par VLAN

ip interface name tunnel @IP_source @IP_dest protocol ipip/gre crée un tunnel

ACL

crée une ACL des @IP à sélectionner
ip access-list nom_ACL address @IP/mask action permit/deny
ou
ip access-list nom_ACL address @IP/mask redist-control all-subnets/no-subnets/aggregate

crée un filtre pour ne laisser passer que les @IP voulues
ip route-map nom_map sequence-number num match-ip-address @IP/mask / nom_ACL permit/deny
ou
ip route-map nom_map sequence-number num match-ip-address @IP/mask / nom_ACL redist-control all-subnets/no-subnets/aggregate

crée un filtre pour ne passer que par le next hop spécifié
ip route-map nom_map sequence-number num match-ip nexthop @IP/mask / nom_ACL permit/deny

Autre méthode

access-list num_ACL permit tcp any any eq smtp
access-list num_ACL permit tcp any any eq 389
access-list num_ACL permit tcp any any eq 123
access-list num_ACL permit tcp any any eq domain
access-list num_ACL permit tcp any any eq www
access-list num_ACL permit tcp any any eq 10319
access-list num_ACL permit tcp any any eq 443
access-list num_ACL permit tcp any any eq 50
access-list num_ACL permit udp any any eq 389
access-list num_ACL permit udp any any eq ntp
access-list num_ACL permit udp any any eq domain

La liste étendue num_ACL permet le passage des flux en sortie des protocoles TCP :

- Messagerie : SMTP -> 25
- Annuaire : LDAP -> 389
- Temps : NTP -> 123
- Domaine : domain/dns -> 53
- Antivirus : tmcm -> 10319 et http : www -> 80
- Cameo : SSL -> 443 pour https

Et des protocoles UDP :

- Annuaire : LDAP -> 389
- Temps : NTP -> 123
- Domaine : domain/dns -> 53,

Depuis et vers n'importe quelle adresse IP.

Autre méthode (plus restrictive)

Pour les flux entrants/sortants de l'interface,

ip access-list extended faslot/port-in/out

Seul l'hôte @IP_2 utilisant les ports serveurs supérieurs à 1023 peut aller vers l'hôte @IP_1 utilisant le port client num_port

remark "commentaire" remark sert pour un commentaire
permit tcp host @IP_2 gt 1023 host @IP_1 eq num_port

Une fois la connexion établie en TCP, seul l'hôte @IP_2 pourra sortir,

remark "established"

permit tcp host @IP_2 any established

Aucune journalisation possible des activités de filtrage de flux,

remark "pas de logs"
deny ip any any log

Commandes d'affichages

show ip config	affiche la configuration des paramètres IP
show ip interface	affiche la configuration IP des interfaces
show ip route	affiche la table de routage
show ip route-pref	affiche les distances administratives par protocole
show ip access-list	affiche les ACL créées
show ip route-map	affiche les conditions de routage des paquets IP
show ip protocols	affiche les protocoles de routage reposant sur IP
show arp	affiche la table de relation entre @MAC et @IP
show tcp/udp ports	affiche les @IP des stations et les ports utilisés

VLAN

vlan id — pour sélectionner un VLAN
vlan id_début-id_fin — pour sélectionner plusieurs VLAN

bridge mode 1x1/flat
1x1 => une instance STP par VLAN / flat => une instance par switch (en option si pas de STP)

vlan id enable/disable name description — crée un VLAN
vlan id port default slot/port | id_aggrégat — assigne un port au VLAN ou un aggrégat de ports
vlan id router ip/ipx @IP @mask forward/no forward e2/snap
configure l'@IP du VLAN, forward => routage ou pas et e2/snap défini le type d'encapsulation
vlan id 802.1Q slot/port | id_aggrégat desc — tagge un port ou un aggrégat de ports
vlan 802.1Q slot/port frame type tagged/all
tagged => seules les trames taggées passent / all => toutes les trames passent
vlan id [1x1/flat] stp enable/disable
active ou désactive le STP sur le VLAN, l'option "1x1 ou flat" est relative au bridge mode
vlan id authentication enable/disable
active l'authentification sur le VLAN et nécessite "aaa authentication vlan" et "avlan ..."
vlan id mtu-ip size
défini la taille en octets de la trame (MTU) contenant un paquet IP

Commandes d'affichages

show vlan — affiche la liste des VLAN
show vlan port — affiche la liste des ports et le VLAN auxquels ils sont assignés
show vlan router ip — affiche la liste des VLAN, leurs @IP et s'ils sont routés
show vlan router mac status
affiche le mode du "router-mac-multiple", la liste des VLAN, leurs @IP et s'ils sont routés
show 802.1Q — affiche l'état du tagging

AGGREGAT DE PORTS

static linkagg id_aggrégat admin state enable/disable — crée un aggrégat de ports
static linkagg id_aggrégat name nom — nomme l'aggrégat
static linkagg id_aggrégat size nbre_ports
définit le nombre de ports dans l'aggrégat
static agg [type_port] slot/port agg num id_aggrégat
assigne un port à un aggrégat, en option le type de port ethernet/fastethernet/gigaethernet

Commandes d'affichages

show linkagg — affiche les aggrégats de ports
show linkagg port — affiche les aggrégats de ports

SNMP

snmp security authentication all
snmp authentication trap enable/disable
snmp community map "nom_map" user "nom_user" on — pour SNMP V1 et V2
snmp trap absorption enable/disable
snmp station @IP port v3 enable/disable user "nom_user" on — par défaut le port est 162

SYSLOG

swlog output console
swlog output flash file-size taille
swlog output flash
swlog output socket @IP_SUPERVISION

ROUTAGE

Statique

ip router primary-address @IP
@IP du routeur ou à défaut celle de la 1°interface sera prise
ip static route @IP @mask gateway @IP_next_hop metric nbre_sauts
défini une route statique
ip route-pref static/ospf/rip valeur — valeur => distance administrative
ip default-ttl nbre_sauts — défini la durée de vie du paquet IP en nombre de sauts

OSPF

ip router router-id @IP
utiliser par OSPF pour déterminer le routeur propageant la Link State DB

ip load ospf — charge le protocole OSPF
ip ospf status enable/disable — active / désactive la configuration d'OSPF
ip ospf area @IP — défini le réseau de l'aire OSPF

Commandes d'affichages

show ip ospf — affiche la configuration d'OSPF

Activer / Désactiver les fonctionnalités et protocoles inutiles

Découverte des équipements adjacents

amap enable/disable	active / désactive AMAP
gmap enable/disable	active / désactive GMAP
amap discovery time sec	intervalle de tps entre chaque envoi de paquets Hello
amap common time sec	intervalle de tps entre chaque réception de paquets Hello

Commandes d'affichages

show amap	affiche l'état du protocole de découverte AMAP
show gmap	affiche l'état du protocole de découverte GMAP

Activer / Désactiver des services

service name	port
ftp	21
ssh	22
telnet	23
http	80
secure-http	443
avlan-http	260
avlan-secure-http	261
avlan-telnet	259
udp-relay	67
network-time	123
snmp	161
avlan-http-proxy	262

ip service nom_service port num active/désactive les services IP

exemple

no ip domain-lookup
ip service snmp
ip service ssh
no ip service ftp
no ip service telnet
no ip service udp-relay
no ip service http
no ip service secure-http
no ip service network-time
no ip service avlan-telnet
no ip service avlan-http
no ip service avlan-secure-http
no ip service avlan-http-proxy
ip service port 1024
ip service port 1025

icmp messages enable/disable — active / désactive ICMP, plus de requêtes ping
icmp type num code num — active / désactive des fonctionnalités ICMP

Message ICMP	Type	Co
réponse à écho	0	0
réseau inaccessible	0	3
hôte inaccessible	3	1
protocole inaccessible	3	2
port inaccessible	3	3
grenade requise mais bit DF spécifié	3	4
échec d'itinéraire source	3	5
réseau de destination inconnu	3	6
hôte de destination inconnu	3	7
hôte source isolé	3	8
Admin du réseau de destination interdit	3	9
admin de l'hôte interdit par un filtre	3	10
réseau inaccessible à TOS	3	11
hôte inaccessible à TOS	3	12
extinction de source	4	0
redirection pour le réseau	5	0
redirection pour l'hôte	5	1
redirection pour TOS et le réseau	5	2
redirection pour TOS et l'hôte	5	3
demande d'écho	8	0
annonce de routeur	9	0
sollicitation de routeur	10	0
temps dépassé lors de la transmission	11	0
temps dépassé lors du réassemblage	11	1
en-tête ip incorrect	12	0
option requise manquante	12	1
demande d'horodateur	13	0
réponse d'horodateur	14	0
demande d'information (obsolète)	15	0
réponse d'information (obsolète)	16	0
demande de masque d'adresse	17	0
réponse de masque d'adresse	18	0