SOMMAIRE

Mode ROMMON

Le mode ROMMON est un IOS simplifié situé dans la ROM. Il est accessible lorsque le switch ne peut pas démarrer, ou si un appui de 5 secondes sur le bouton "mode" interrompt la séquence de boot normale.

Transfert XMODEM

switch : flash_init — initialise la mémoire flash
switch : dir flash : — liste la mémoire flash

Configurez les variables d'environnement pour le transfert série

switch : set NOM_VARIABLE VALEUR — configure une variable
switch : unset NOM_VARIABLE VALEUR — efface une variable

switch : set BAUD 115200

Note : Changez la vitesse de votre émulateur de terminal à 115200

switch : copy xmodem: NOM_IOS.bin flash:NOM_IOS.bin

Envoyez le fichier via votre émulateur de terminal

Attention : N'oubliez pas de reconfigurer le port console à 9600 bauds ainsi que le nom de l'IOS à charger au démarrage si besoin !!

switch : set BAUD 9600
switch : set BOOT flash:NOM_IOS.bin

switch : boot — relance la séquence de démarrage

Mode privilégié

Note : à la question "Souhaitez-vous entrer dans le dialogue de configuration initiale ?"
répondez "non"

à la question "Souhaitez-vous terminer l'installation automatique ?"
répondez "yes" ou tapez ENTREE

```
Switch>enable
        ou
Switch>enable level
Password: mdp / rien ou cisco par défaut
Switch#
Switch#disable
Switch>
```

Manipuler les fichiers

```
Switch#cd ..            accès au dossier parent
Switch#dir              pour lister le contenu d'un répertoire
Switch#dir system:      pour voir la RAM (memory, running-config…)
Switch#dir nvram:       pour voir la NonVolatileRAM (startup-config…)
Switch#dir flash:       pour voir la mémoire flash (IOS…)

Switch#rename ancien_nom nvo_nom                renommer
Switch#delete nom_fichier                       effacer un fichier
Switch#delete /recursive /force nom_dossier     effacer un dossier
Switch#erase nom_fichier_systeme
Switch#more nom_fichier                         effacer un dossier
```

Remettre en configuration usine

```
Switch#write erase
        ou
Switch#erase startup-config
Switch#dir
Switch#cd flash:        pour se positionner dans la flash (optionnel si vlan.dat déjà listé)
Switch#delete vlan.dat  puis tapez sur ENTREE, puis ENTREE pour confirmer
Switch#dir              nettoyer les fichiers inutiles si nécessaire
Switch#reload
```

Note : à la question "Souhaitez-vous enregistrer la configuration", répondez "non"

Sauvegarder / Restaurer la configuration / l'IOS

```
Switch#write
        ou
Switch#copy running-config startup-config                dans la mémoire persistante
Switch#copy running-config ftp://@SVR_TFTP/sauvegarde    sur serveur TFTP
Switch#copy ftp://@SVR_FTP/sauvegarde startup-config     depuis serveur FTP
Switch#copy ftp://@SVR_FTP/c1700.bin flash:              IOS depuis serveur FTP

Switch(config)#archive
Switch(config-archive)#path flash:                       sauvegarde en local
Switch (config-archive)#path tftp://SVR-TFTP//$h.cfg     sauvegarde sur serveur TFTP
Switch (config-archive)#path scp://USER :MDP@SVR-SCP//$h.cfg
SCP = Secure Copy Protocol, protocole utilisant SSH port 22
USER = compte local existant sur SVR SCP
MDP = mot de passe associé au compte
$h = variable d'environnement équivalent au hostname de l'EAR
Switch(config-archive)#maximum nbre_backupnbre de sauvegardes conservées
Switch(config-archive)#write-memory              crée sauvegarde si enregistrement
Switch(config-archive)#time-period 1440 (en min) crée sauvegarde toutes les 24H

Switch#archive config                                    lance une sauvegarde
Switch#configure replace scp://USER :MDP@SVR-SCP//$h.cfg restaure une sauvegarde
```

Redémarrer

```
Switch#reload                    redémarrage immédiat
Switch#reload at hh:mm
Switch#reload in mm ou hh:mm     compte à rebours
```

Paramétrer l'heure

```
Switch#clock set hh :mm :ss jj MONTH yyyy
```

Réinitialisation de paramétres

```
Switch#clear mac-address-table   vide la table d'@MAC
Switch#clear arp-cache           vide le cache des relations @MAC/@IP
Switch#clear ip route *          vide la table de routage
```

Visualisation des configurations et états

Switch#show running-config	config courante en RAM
Switch#show startup-config	config persistante en NVRAM
Switch#show config id detail	affiche les infos du dernier enregistremt de la conf
Switch#show version	affiche la version de l'IOS
Switch#show logging	affiche l'état de la journalisation
Switch#show vlan brief	affiche les VLANs et leurs ports assignés
Switch#show vlan private-vlan type	affiche les PVLANs et leur type
Switch#show mac-address-table	affiche la table d'@MAC
Switch#show port-security	affiche l'état de la sécurité
Switch#show arp	affiche la table de relation @MAC et @IP
Switch#show ip interface brief	affiche l'état et l'@IP de toutes les interfaces
Switch#show interface description	affiche l'état et la desc de toutes les interfaces
Switch#show interfaces status	affiche l'état et le nom de toutes les interfaces
Switch#show protocols	affiche l'état et l'@IP de toutes les interfaces
Switch#show ip route	affiche la table de routage
Switch#show archive config	affiche les sauvegardes effectuées
Switch#show authentication sessions	affiche les clients authentifiés en 802.1X
Switch#show dot1x all summary	affiche l'état des ports 802.1X

Mode de configuration globale

```
Switch#configure terminal
Switch(config)#
```

Nommer le switch

```
Switch(config)#hostname nom_switch
```

Afficher une bannière

```
Switch(config)#banner motd ^

        Message Of The Day
^
Switch(config)#banner login ^

        NOM DU SWITCH
^
Switch(config)#banner @
        +---------------------------------------------------------------------------+
        &                          RESEAU CLASSIFIE                                 &
        +---------------------------------------------------------------------------+
        &                                                                           &
        &  TOUT ACCES NON AUTORISE EST ENREGISTRE ET PUNI PAR LA LOI                 &
        &                                                                           &
        +---------------------------------------------------------------------------+
        &                          CLASSIFIED NETWORK                               &
        +---------------------------------------------------------------------------+
        &                                                                           &
        &   UNAUTHORIZED ACCESS WILL BE LOGGED AND TAKEN TO COURT                   &
        &                                                                           &
        +---------------------------------------------------------------------------+
@
```

Le caractère qui délimite le texte de la bannière doit être identique au début et à la fin de celle-ci. Ici c'est le '@'

Activer routage inter-VLANs

```
Switch(config)#ip routing                    passage en niv 3 => routage inter-vlan
```

Configurer la passerelle sur le SW

```
Switch(config)#ip default-gateway @IP        modèle 2900
```

!! Attention : ip routing ne doit pas être activé !!

Activer le chiffrement de type 7 (propriétaire CISCO)

Switch(config)#service password-encryption chiffre les mdp des accès console, vty …
Switch(config)#no service password-recovery
!! modification du mdp et/ou récupération de la configuration impossible lors du break durant le boot, seule la remise en configuration usine est possible !!

Protéger le mode privilégié par mdp

Switch(config)#enable password mdp mdp enregistré en clair
Switch(config)#enable secret mdp mdp enregistré avec chiffrement type 5 (hash MD5)
ou
Switch(config)#enable secret level level mdp si gestion des niveaux de privilège

Verrouillage session

Switch(config)#login block-for duree_verrouillage attempts tentatives within periode
Durée verrouillage (sec) / Période (sec) durant laquelle les tentatives sont prises en compte
Attention : le verrouillage s'applique à tous les comptes en plus de celui incriminé

Créer un utilisateur

Switch(config)#username nom_user privilege niveau password num mdp mdp en clair
Switch(config)#username nom_user privilege niveau secret num mdp mdp en MD5

privilége 0 => utilisateur | accès possible mode privilégié
privilége 1 => utilisateur / visualisateur (sauf config) | accès possible mode privilégié
privilége 2 à 14 => utilisateur / visualisateur (sauf config) | accès direct mode privilégié puis accès possible au mode de configuration globale
privilége 15 => administrateur | accès possible au mode de configuration globale

Switch(config)#privilege exec level niveau commande
assigner des droits à un niveau de privilège / exec = pour mode privilégié
Switch(config)#privilege exec reset commande
restaurer les droits par défaut

Switch(config)#security passwords min-length num num = longueur du mdp (mettre 14)

Activer / Désactiver les fonctionnalités et protocoles inutiles

```
Switch(config)#no cdp run                  pas de CISCO Discovery Protocol
Switch(config)#no ip cef                   pas de CISCO Express Forwarding
Switch(config)#no ip domain-lookup         pas joindre DNS en broadcast si commande erronée
Switch(config)#no ip bootp server          pas de chargement d'IOS à distance
Switch(config)#no ip http server           pas de serveur HTTP
Switch(config)#no ip http secure-server pas de serveur HTTPS
Switch(config)#no ip snmp-server
        ou                                 pas de serveur SNMP
Switch(config)#no snmp-server
Switch(config)#no ip classless             pas d'@mask raccourcies = pas de CIDR
Switch(config)#no ip subnet-zero           pas de sous RSO en 0
Switch(config)#no ip routing               désactive le routage inter-VLAN
Switch(config)#no ip dhcp server
        ou                                 pas de serveur DHCP
Switch(config)#no service dhcp
Switch(config)#no ip classless             prise en compte des classes d'@IP = pas de CIDR
Switch(config)#no ip subnet-zero           pas de sous RSO en 0
Switch(config)#no service tcp-small-servers
Switch(config)#no service udp-small-servers
Switch(config)#no service config           pas de chargement de fichier de config à distance
Switch(config)#no ip finger
Switch(config)#no service finger           liste les utilisateurs connectés
Switch(config)#no ip source-route          pas de contournements des règles de routage
Switch(config)#no service pad              pas de Packet Assembler Disassembler
Switch(config)#no ip ftp passive           le client FTP ne décide pas du port à utiliser
Switch(config)#no spanning-tree vlan id_vlan
désactive le Spanning-Tree Protocol
Switch(config)# vtp mode off | transparent
pas de VLAN Trunking Protocol | laisse passer les trames VTP sans màj de sa base de VLANs
permet l'affichage de la VLAN database dans la configuration
Switch(config)#no tftp-server flash:
```

Spanning-Tree Protocol

Une topologie redondante provoque :

- des orages de broadcasts (trame infinie surcharge matérielle)
- des duplications de trames
- des tables MAC instables

Le STP est un protocole qui permet de résoudre les problèmes liés à une topologie redondante. Il supprime de manière logique les boucles physiques.

Switch(config)#spanning-tree vlan ID-VLAN priority MULTIPLE-de-4096
définit la priorité du SWITCH (pour calcul du bridge ID)

Switch(config)#interface fastethernet|gigabitethernet slot/port
Switch(config-if)#spanning-tree vlan ID-VLAN port-priority MULTIPLE-de-16
définit la priorité du port

Switch(config-if)#spanning-tree bpduguard disable
Switch(config-if)#spanning-tree bpdufilter disable
désactive le STP sur les ports reliés à des EAR ne participant pas au STP

Switch(config)# spanning-tree mode pvst (répartition de charge) | mst | rapid-pvst
PVST = Per-Vlan Spanning-Tree >> 1 instance par VLAN
MST = Multiple Spanning-Tree >> 1 instance pour tous les VLANs

Authentication Authorization Accounting

Activation AAA

```
Switch(config)#aaa new-model
```
active les fonctionnalités AAA = Authentication/Authorization/Accounting

Gestion des droits d'accès par VIEW

```
Switch(config)#parser view NOM-VUE
Switch(config-view)#secret MDP
```
création de la vue

```
Switch(config-view)#commands exec include all show
Switch(config-view)#commands exec exclude all clear
Switch(config-view)#commands configure include all snmp-server
Switch(config-view)#commands configure include all logging
Switch(config-view)#commands configure exclude all router
```
paramètrage des commandes accessibles ou non

```
Switch(config-view)#exit
```

Affecter la VIEW

```
Switch(config)#username nom_user view NOM-VUE secret|password mdp
```

AAA et 802.1X avec RADIUS

Activation AAA

```
Switch(config)#aaa new-model
```
active les fonctionnalités AAA = Authentication/Authorization/Accounting

Configuration des serveurs RADIUS

```
Switch(config)#ip radius source-interface fastethernet|gigabitethernet|vlan slot/port|num
Switch(config)#radius-server host @IP_SVR-RADIUS auth-port 1812 acct-port 1813 key mdp
```
Paramètrage du serveur RADIUS à joindre :

timeout	= tps d'attente de la réponse du serveur	
retransmit	= nbre de tentatives de communication avec le serveur	
auth-port	= port UDP dédié à l'authentification (par défaut 1645)	optionnel
acct-port	= port UDP dédié à l'accounting (par défaut 1646)	optionnel

Configuration de l'authentification

```
Switch(config)# aaa authentication username-prompt " ENTREZ VOTRE IDENTIFIANT : "
Switch(config)# aaa authentication password-prompt " ENTREZ VOTRE MOT DE PASSE : "
Switch(config)# aaa authentication fail-message " !! ACCES REFUSE !! "
Switch(config)# aaa authentication attempts login 3
```

Switch(config)#aaa authentication login default|nom_liste_authentif_CONSOLE line
Utilise le mdp de l'interface de connexion (console, vty …)
Switch(config)#aaa authentication login default|nom_liste_authentification group radius local
Utilise les serveurs RADIUS puis les comptes locaux si SVR injoignable
Switch(config)#aaa authentication ppp default|nom_liste_authentif_PPP group radius local
L'authentification PPP utilise les serveurs RADIUS puis les comptes locaux si SVR injoignable
Switch(config)#aaa authentication enable default radius enable
Utilise les serveurs RADIUS (*créer le compte $enab15$ au préalable sur SVR RADIUS avec un mdp*), puis le mot de passe 'enable' si SVR injoignable

NOTE : La liste "default" affecte ttes les interfaces de connexion
≠ liste "nom_liste_authentification"

Configuration de l'autorisation

Switch(config)#aaa authorization exec default|nom_liste_authorization group radius local
Le serveur RADIUS est configuré tel que : Service-Type=1 ou Login
accès direct au mode privilégié quand le SVR RADIUS affecte des droits >1 à l'utilisateur
ex attributs spécifiques CISCO : shell:priv-lvl=15
Switch(config)#aaa authorization network default|nom_liste_authoriz_PPP group radius local
spécifie si les utilisateurs ont accès aux services réseaux type PPP ou SLIP
Le serveur RADIUS est configuré tel que : Service-Type=7 ou PPP
Switch(config)#aaa authorization console
Active l'utilisation de la liste "nom_liste_authorization" dans line console 0

NOTE : La liste "default" affecte ttes les interfaces de connexion
≠ liste "nom_liste_authorization"

Application des paramètres AAA

Switch(config)#line con 0
Switch(config-line)#password MDP
Switch(config-line)#authorization exec default|nom_liste_authorization
Switch(config-line)#login authentication default|nom_liste_authentif_CONSOLE

Switch(config)#line vty 0
Switch(config-line)#authorization exec default|nom_liste_authorization
Switch(config-line)#login authentication default|nom_liste_authentification

Switch(config)#line serial|dialer 0
Switch(config-if)#ppp authorization default|nom_liste_authoriz_PPP
Switch(config-if)#ppp authentication chap|pap|ms-chap-v2
default|nom_liste_authentif_PPP

Configuration de 802.1X

Switch(config)#aaa authentication dot1x default group radius
Utilise les serveurs RADIUS pour l'authentification 802.1X
Switch(config)#aaa authorization network default group radius
Les serveurs RADIUS définissent le niveau d'autorisation appliquée à la demande d'accès rso

NOTE : La liste "default" affecte ttes les interfaces de connexion

Switch(config)#dot1x system-auth-control

Application des paramètres 802.1X

Switch(config)#interface fastethernet|gigabitethernet slot/port
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#authentication event no-response action authorize vlan num
clients non compatibles 802.1X => assignation dans vlan invité (cas des imprimantes, tv …)
Switch(config-if)#authentication event fail action authorize vlan num
échec d'authentification du client => vlan poubelle

Fonctions de test AAA et 802.1X

Switch#test aaa group radius NOM-USER MDP legacy

Switch#dot1x test eapol-capable interface ethernet slot/port
Switch#dot1x initialize interface ethernet slot/port
Switch#dot1x re-authenticate interface ethernet slot/port

SNMP (Simple Network Management Protocol) V2c/V3

[Switch(config)#snmp-server engineId id_agent] défini le nom de l'agent [optionnel]

Pour la version V2c (c pour communauté pas chiffrement)
Switch(config)#snmp-server community nom_communauté RO|RW nom_ACL

Pour la version V3
Switch(config)#snmp-server group nom_grp v3 auth [access nom_ACL]
groupe avec autorisation seulement [optionnel, applicable au user SNMP]
Switch(config)#snmp-server user user nom_grp v3 auth md5|sha mdp
défini l'utilisateur autorisé

Switch(config)#snmp-server host @IP_SUPERVISION version 3 auth user
Switch(config)#snmp-server host @IP_SUPERVISION informs version 3 auth user
Switch(config)#snmp-server host @IP_SUPERVISION traps version 3 auth user
défini la station de supervision à joindre pour l'utilisateur SNMP V3 créé

ou (l'activation du chiffrement = privacy, dépend de l'IOS)

Switch(config)#snmp-server group nom_grp v3 priv [access nom_ACL]
groupe avec privacy [optionnel, applicable au user SNMP]
Switch(config)#snmp-server user user nom_grp v3 auth md5/sha mdp priv des|aes 128 mdp
défini l'utilisateur autorisé avec privacy

Switch(config)#snmp-server host @IP_SUPERVISION version 3 priv user
Switch(config)#snmp-server host @IP_SUPERVISION informs version 3 priv user
Switch(config)#snmp-server host @IP_SUPERVISION traps version 3 priv user
défini la station de supervision à joindre pour l'utilisateur SNMP V3 créé

Switch(config)#snmp-server source-interface traps vlan ID_VLAN
Switch(config)#snmp-server source-interface informs vlan ID_VLAN

Switch(config)#snmp-server manager gestionnaire SNMP
Switch(config)#snmp-server location nom_lieu
Switch(config)#snmp-server contact nom_contact-TEL

Restrictions SNMP
Switch(config)#snmp-server view nom_VIEW_A OID included|excluded
Switch(config)#snmp-server view nom_VIEW_B OID included|excluded
Switch(config)#snmp-server view nom_VIEW_C OID included|excluded

Switch(config)#snmp-server group nom_grp_A v3 auth|priv read nom_VIEW_A
Switch(config)#snmp-server group nom_grp_B v3 auth|priv write nom_VIEW_B
Switch(config)#snmp-server group nom_grp_C v3 auth|priv notify nom_VIEW_C

```
Switch(config)#snmp-server enable traps                    active toutes les notifications
Switch(config)#snmp-server enable traps config             configuration modifiée
Switch(config)#snmp-server enable traps config-copy
Switch(config)#snmp-server enable traps config-ctid
Switch(config)#snmp-server enable traps syslog             SYSLOG
Switch(config)#snmp-server enable traps tty                accès SSH/TELNET
Switch(config)#snmp-server enable traps authenticate-fail  authentifications ratées
Switch(config)#snmp-server enable traps envmon             notifications matérielles
Switch(config)#snmp-server enable traps memory bufferpeak
Switch(config)#snmp-server enable traps event-manager
Switch(config)#snmp-server enable traps cpu threshold
Switch(config)#snmp-server enable traps flash insertion removal
Switch(config)#snmp-server enable traps vlancreate
Switch(config)#snmp-server enable traps vlandelete
Switch(config)#snmp-server enable traps vlan-membership
Switch(config)#snmp-server enable traps mac-notification
Switch(config)#snmp-server enable traps port-security
Switch(config)#snmp-server enable traps auth-framework sec-violation

nettoyage des groupes et utilisateurs SNMP générés automatiquement
Switch(config)#no snmp-server group ILMI v1
Switch(config)#no snmp-server group ILMI v2C
Switch(config)#no snmp-server group NOM_GROUP v3 priv

CTRL+Z pour retour au mode privilégié
```

Journalisation en LOCAL / vers SYSLOG

```
Switch(config)#service timestamps debug datetime    datation de la journalisation
Switch(config)#service timestamps log datetime      datation de la journalisation

Switch(config)#logging @IP                          @IP du serveur SYSLOG
Switch(config)#logging host @IP                     @IP du serveur SYSLOG

Switch(config)#logging buffered taille_tampon       journalisation locale
Switch(config)#logging console warnings             niv de journalisation vers la console
Switch(config)#logging monitor informational        niv de journalisation vers les VTY
Switch(config)#logging trap debugging               niv de journalisation vers SYSLOG
Switch(config)#logging cns-events emergency
Switch(config)#logging origin-id string hostname    entête des logs
        ou
Switch(config)#logging origin-id hostname           entête des logs
Switch(config)#logging source-interface nom_interface slot/port
Switch(config)#logging userinfo                     enregistre les infos de connexion
Switch(config)#login on-failure log
Switch(config)#login on-success log
Switch(config)# logging count
Switch(config)#logging on                           active l'envoi des logs
```

Enregistrement des changements de configuration

```
Switch(config)#archive
Switch(config-archive)#log config
enregistre les modifs de la running-config = commandes tapées
Switch(config-archive-log-cfg)#hidekeys             empêche l'affichage en clair des mdp
Switch(config-archive-log-cfg)#notify syslog        déport SYSLOG des commandes tapées
Switch(config-archive-log-cfg)#logging size num     num = 1000 par exemple
Switch(config-archive-log-cfg)#logging enable
active la journalisation des commandes tapées dans le CLI
```

Filtrage des remontées SYSLOG

```
Switch(config)# logging discriminator NOM_FILTRE msg-body drops "logged command"
exemple de filtre empêchant la remontée d'informations concernant les commandes tapées
Switch(config)# logging host @IP discriminator NOM_FILTRE
```

NTP = Network Time Protocol

```
Switch(config)#interface nom_interface slot/port
Switch(config-if)#no ntp disable
exit

Switch(config)#ntp logging                                  active les logs NTP
Switch(config)#ntp authenticate
Switch(config)#ntp authentication-key num_clé md5 mdp
Switch(config)#ntp trusted-key num_clé
Switch(config)#ntp update-calendar
```

à paramétrer sur l'EAR faisant office de serveur NTP :

```
Switch(config)#ntp server master num_stratum
```

num_stratum = niveau hiérarchique du serveur dans l'architecture des synchronisations

à paramétrer sur l'EAR client du serveur NTP :

```
Switch(config)#ntp server @NTP_SERVER source nom_interface slot/port key num_clé
version X
```

@IP du serveur de temps de référence

Monitoring de port / VLAN

```
Switch(config)# monitor session num source interface fastethernet slot/port both
        ou
Switch(config)# monitor session num source vlan id_vlan
Switch(config)# monitor session num destination interface fastethernet slot/port
Switch(config)# monitor session num destination int eth slot/port replicate encapsulation
```

Permet la capture du TAG

```
Switch(config)# monitor session num filter vlan id_vlan       filtre par VLAN
```

Les Access List -> ACL

liste d'accès standard -> n° d'ACL allant de 1 à 99

Switch(config)#access-list num_ACL permit / deny @source
n° d'ACL correspond à n° d'access-group

exemples :

Switch(config)#access-list 1 permit 192.168.100.0 0.0.0.255 attention : masq_inversé
Switch(config)#access-list 2 deny host 192.168.100.200 0.0.0.0 ici le masq est inutile
Switch(config)#access-list 3 permit any tout traffic est autorisé

Switch(config-if)#ip access-group num_ACL in / out traffic entrant / sortant
n° d' access-group correspond à n° d' ACL

Switch(config-line)#access-class num_ACL in / out traffic entrant / sortant
n° d' access-class correspond à n° d' ACL

liste d'accès étendue -> n° d'ACL allant de 100 à 199

Switch(config)#access-list num_ACL permit / deny protocole @source @destination
n° d'ACL correspond à n° d'access-group

exemples :

Switch(config)#access-list 167 deny tcp any any eq 67
Switch(config)#access-list 168 deny tcp any any eq 68
Switch(config)#access-list 167 deny udp any any eq 67
Switch(config)#access-list 168 deny udp any any eq 68
pas de bootp depuis tous les RSO vers tous les RSO

Switch(config)#access-list 121 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 21
pas de ftp depuis RSO 192.168.1.0 vers RSO 192.168.2.0 / attention : masq_inversé

Switch(config)#access-list 123 permit tcp host 192.168.10.20 host 10.2.0.120 eq 23
telnet autorisé depuis 192.168.10.20 vers 10.2.0.120 / ici le masq est inutile

Switch(config)#access-list 101 permit ip any any
tout le reste du traffic est autorisé

Switch(config-if)#ip access-group num_ACL in / out traffic entrant / sortant
n° d' access-group correspond à n° d' ACL

!!! Attention: Une ACL a comme dernière règle de filtrage un "deny any" implicite.
Pour modifier une ACL, il est d'abord nécessaire de la supprimer puis de la réinsérer entièrement avec les modifications souhaitées, sauf si utilisation des numéros de séquence !!! *

CTRL+Z pour retour au mode privilégié

Les VLAN Access List -> VACL

cibler les flux souhaités
Switch(config)#ip access-list extended VACL-VID
Switch(config-ext-nacl)#permit ip host @IP-A host @IP-B
Switch(config-ext-nacl)#permit ip host @IP-B host @IP-A
Switch(config-ext-nacl)#deny ip any any
Switch(config-ext-nacl)#exit

créer la VACL qui permet ou interdit les flux ciblés
Switch(config)#vlan access-map VMAP-VACL-VID [n°séquence] optionnel (10 par défaut)
Switch(config-access-map)#match ip address VACL-VID
Switch(config-access-map)#action drop
les flux ciblés par l'ACL sont interdits
Switch(config-access-map)#exit

ATTENTION : Comme pour les route-map il existe un drop implicite en séquence finale

Switch(config)#vlan access-map VMAP-VACL-VID n°séquence ici, séquence 20 par ex
Switch(config-access-map)#action forward
les autres flux sont autorisés
Switch(config-access-map)#exit

appliquer la VACL à un VLAN, ou à plusieurs
Switch(config)#vlan filter VMAP-VACL-VID vlan-list VID

Mode de configuration spécifique

mode ligne pour les interfaces de connexion au switch

```
Switch(config)#line console 0      pour le port série
Switch(config)#line aux 0          pour le port auxiliaire -> télégestion par modem
Switch(config)#line vty 0 4        pour les terminaux virtuels -> telnet
Switch(config)#line slot/port      pour les modems
```

Configurer le port console

```
Switch (config)#line console 0
Switch(config-line)#logging synchronous                 enlève les affichages perturbateurs
Switch(config-line)#exec-timeout minutes secondes
Switch(config-line)#login          si authentification simple-> c le password qui est utilisé
Switch(config-line)#login local    si authentification locale -> comptes utilisateurs utilisés
Switch(config-line)#login authentication default|nom_liste_authentification
                                   si authentification RADIUS -> comptes SAM|AD utilisés
Switch(config-line)#password MDP
Switch(config-line)#exit
```

Désactiver port auxiliaire

```
Switch(config)#line aux 0
Switch(config-line)#login
Switch(config-line)#no password
Switch(config-line)#no exec
Switch(config-line)#exec-timeout 0 1
Switch(config-line)#transport input none
Switch(config-line)#transport output none
Switch(config-line)#transport preferred none
Switch(config-line)#exit
```

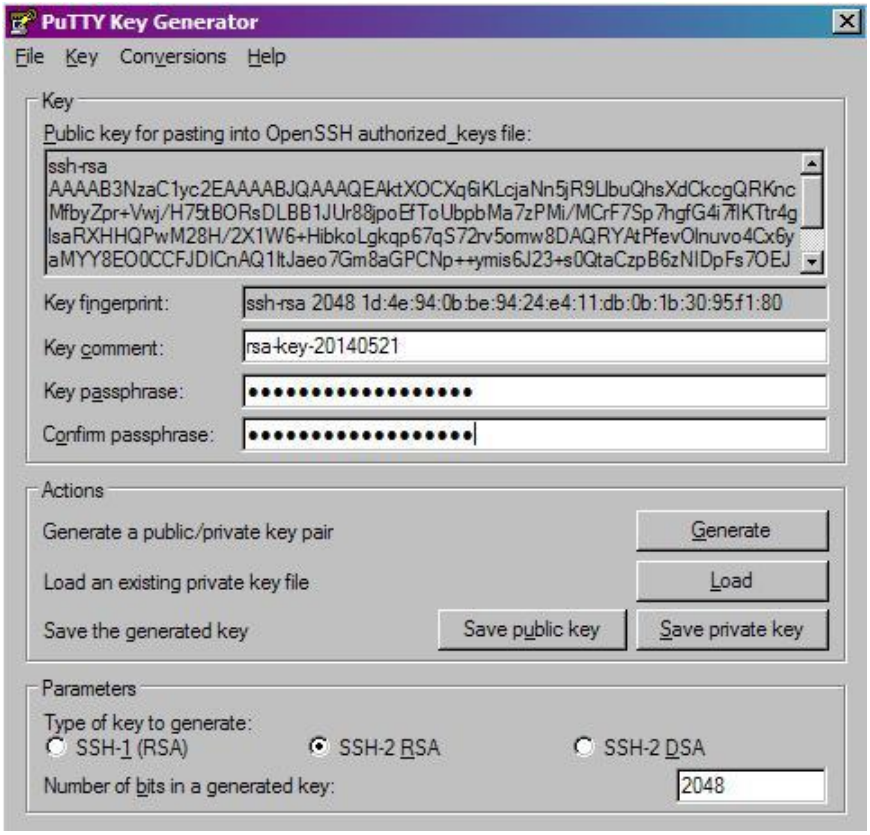
VTY -> TELNET

```
Switch(config)#ip telnet source-interface vlan ID_VLAN

Switch(config)#line vty 0 4
Switch(config-line)#exec-timeout minutes secondes
Switch(config-line)#login                 si authentification simple-> c le password qui est utilisé
Switch(config-line)#login local           si authentification locale -> comptes utilisateurs utilisés
Switch(config-line)#login authentication default|nom_liste_authentification
                                          si authentification RADIUS -> comptes SAM|AD utilisés
Switch(config-line)#password mdp
Switch(config-line)#transport input telnet
Switch(config-line)#transport output telnet
Switch(config-line)#transport preferred telnet
Switch(config-line)#monitor
active jusqu'à la déconnexion l'affichage des messages de la console vers l'interface vty
Switch(config-line)#exit
```

VTY -> SSH = Secure SHell

```
Switch(config)#ip ssh version num_version
Switch(config)#ip ssh time-out secondes                tps donné pour se connecter (60 sec)
Switch(config)#ip ssh authentication-retries num       mettre 3
Switch(config)#ip ssh source-interface vlan ID_VLAN
Switch(config)#ip ssh logging events                   log des connexions SSH
Switch(config)#ip domain-name nom_domaine              exemple -> nom_domaine = NOM_RSO
Switch(config)#crypto key generate rsa modulus 2048
        ou
Switch(config)#ip ssh pubkey-chain
Switch(conf-ssh-pubkey)#username nom_user
c'est la passphrase associée à la clé qui sera demandée lors de la connexion de cet
utilisateur
Switch(conf-ssh-pubkey-user)#key-string
```



Switch(conf-ssh-pubkey-data)#clé_publique exemple -> AAAAB.....aaa==
coller la clé publique générée avec PUTTYGEN, si trop longue, coller les segments de la clé séparés par des / les uns après les autres
Switch(conf-ssh-pubkey-data)#exit
Switch(conf-ssh-pubkey-user)#exit
Switch(conf-ssh-pubkey)#exit

Switch(config)#line vty 0 4
Switch(config-line)#exec-timeout minutes secondes
Switch(config-line)#login si authentification simple-> c le password qui est utilisé
Switch(config-line)#login local si authentification locale -> comptes utilisateurs utilisés
Switch(config-line)#login authentication default|nom_liste_authentification
si authentification RADIUS -> comptes SAM|AD utilisés
Switch(config-line)#password mdp
Switch(config-line)#transport input ssh
Switch(config-line)#transport output ssh
Switch(config-line)#transport preferred ssh
Switch(config-line)#monitor
active jusqu'à la déconnexion l'affichage des messages de la console vers l'interface vty
Switch(config-line)#exit

mode vlan

Création de VLAN

Note: Gestion des VLANs de manière statique

```
Switch#vlan database
Switch(vlan)#vlan num_vlan enable|disable name nom_vlan      nomme le VLAN
Switch(vlan)#vlan num_vlan state active|suspend              active/désactive le VLAN
```

ou

```
Switch(config)#vlan num_vlan
Switch(config-vlan)#name nom_vlan                    nomme le VLAN
Switch(config-vlan)#state active|suspend             active / désactive le VLAN
```

Assigner des ports à un VLAN …

VLAN Trunking Protocol

Note: Gestion des VLANs de manière dynamique
Nécessite que les ports d'interconnexion soient trunkés

```
Switch(config)#vtp mode server
Switch(config)#vtp domain NOM-DOMAINE-VTP
Switch(config)#vtp password MDP
Switch(config)#vtp version 1 | 2 | 3

Switch(config)#vtp pruning
```

désactive l'envoi des trames appartenant à un VLAN vers un switch n'utilisant pas ce VLAN
à activer sur le switch serveur, maître des échanges VTP

```
Switch(config)#vtp mode client
Switch(config)#vtp password MDP

Switch(config)# vtp mode transparent
```

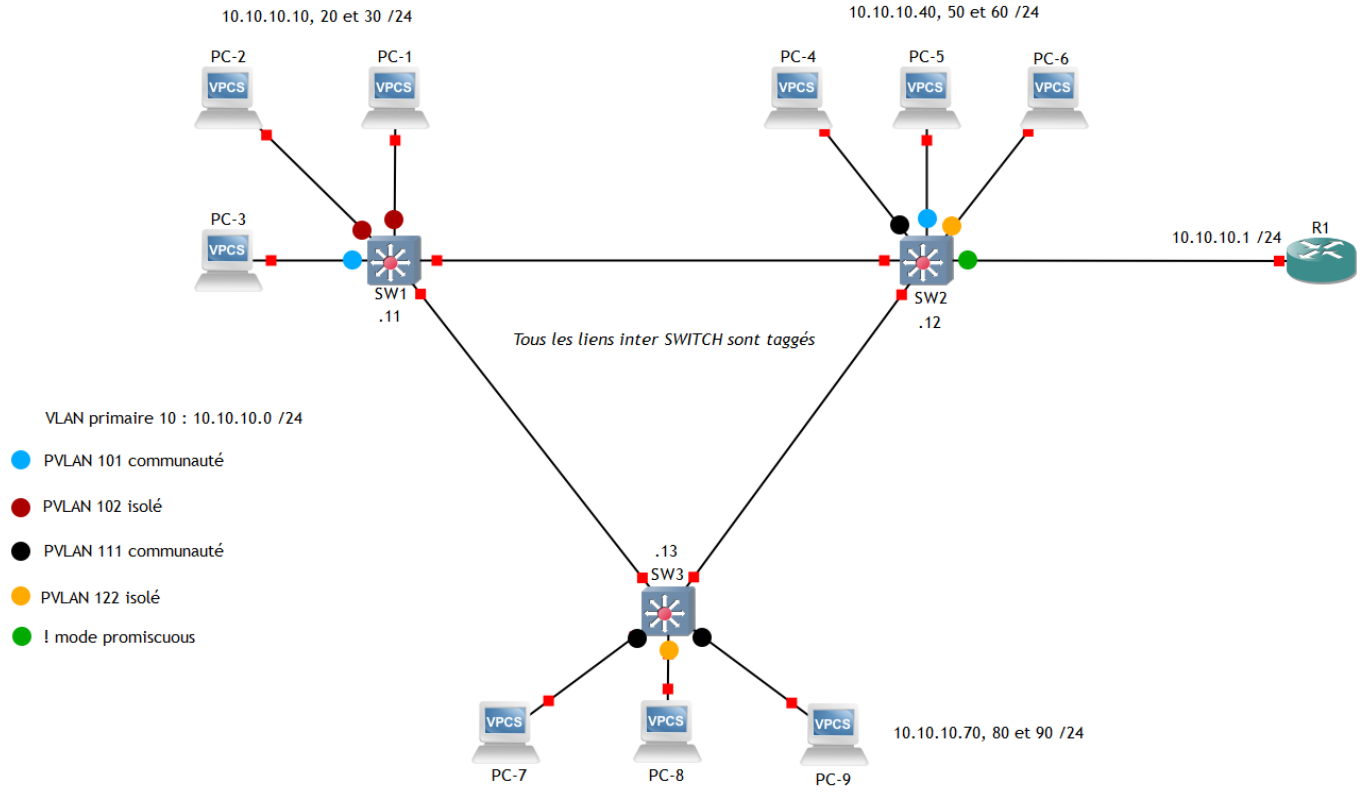
le switch laisse passer les trames VTP sans màj de sa propre base de VLANs
permet l'affichage de la VLAN database dans la configuration

```
Switch#show vtp status
```

Private VLAN

Les Private VLAN permettent de créer des sous-domaines de diffusion au sein d'un premier PVLAN commun, le PVLAN primaire. Ces sous-domaines sont le résultat de l'utilisation de PVLAN secondaires rattachés au primaire.

ATTENTION : l'utilisation des PVLAN nécessite que VTP soit désactivé !



création PVLAN primaire

```
Switch(config)#vlan ID_VLAN_PRIMAIRE
Switch(config-vlan)#private-vlan primary
```

création PVLAN secondaire

Création d'un PVLAN secondaire de type communauté

```
Switch(config)#vlan ID_VLAN_COM
Switch(config-vlan)#private-vlan community
```

Création d'un PVLAN secondaire de type isolé

```
Switch(config)#vlan ID_VLAN_ISOLE
Switch(config-vlan)#private-vlan isolated
```

Association des PVLAN secondaires au primaire

```
Switch(config)#vlan ID_VLAN_PRIMAIRE
Switch(config-vlan)#private-vlan association ID_VLAN_COM,ID_VLAN_ISOLE,ID_VLAN_COM
```

Note: on peut associer plusieurs PVLAN communauté au primaire, mais qu'un seul isolé

PVLAN - Assignation

Assignation d'un port à un PVLAN secondaire
Switch(config)#interface fastethernet slot/port
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association ID_VLAN_PRIMAIRE ID_VLAN_COM

Configuration d'un port en mode promiscuous
Switch(config)#interface fastethernet slot/port
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping ID_VLAN_PRIMAIRE ID_VLAN_COM, ID_VLAN_ISOLE,ID_VLAN_COM

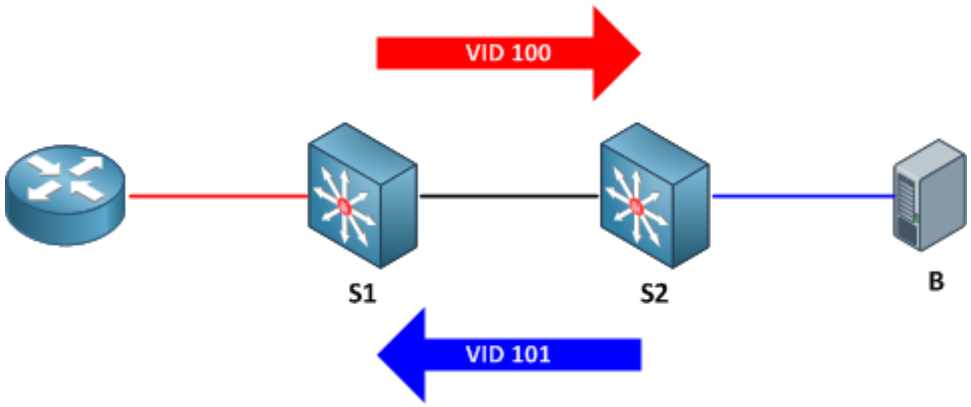
Bilan:

- les stations appartenant à un PVLAN isolé ne commmuniquent pas entre elles, mais avec ! promiscuous
- les stations appartenant à un PVLAN communauté commmuniquent entre elles, et avec ! promiscuous, mais pas avec les stations appartenant à un autre PVLAN secondaire

- le STP fonctionne de la même façon, en mode PVST, une instance par PVLAN

- le TAG des trames provenant des stations a pour VID celui du PVLAN auquel elles appartiennent
- le TAG des trames provenant du routeur connecté au ! en mode promiscuous, a pour VID celui du PVLAN primaire

exemple de TAG :



mode interface pour les ports du switch (fastethernet,VLAN,loopback…)

Switch(config)#interface loopback num_interface_virtuelle
Switch(config)#interface fastethernet slot/port
Switch(config)#interface gigabitethernet slot/port

Mettre une @IP sur une interface

Switch(config-if)#no switchport
enlève le port de tous les VLANS même le VLAN par défaut
si le port appartient à un VLAN, c'est l'@IP du VLAN qui prime
Switch(config-if)#ip address @IP @mask seulement si "no switchport"
Switch(config-if)#ip address @IP @masque secondary
2°@IP pour un port switché en no switchport /préférer les sous-interfaces pour les ports routés
Switch(config-if)#ip address dhcp attribution dynamique d'une @IP par SVR DHCP

Mettre une @IP sur un VLAN

Switch(config)#interface vlan num_vlan
Switch(config-if)#ip address @IP @mask
Switch(config-if)#management pour le VLAN d'ADMINISTRATION sur 2900 series

NETTOYAGE DES INTERFACES VLAN

Switch(config-if)#no ip proxy-arp	désactive le proxy ARP *
Switch(config-if)#no ip local-proxy-arp	désactive le proxy ARP *
Switch(config-if)#no ip rarp-server	désactive le Relais ARP
Switch(config-if)#no ip redirects	désactive un outil du protocole ICMP
Switch(config-if)#no ip unreachables	désactive un outil du protocole ICMP
Switch(config-if)#no ip mask-reply	désactive un outil du protocole ICMP
Switch(config-if)#no ip route-cache	désactive l'enregistrement d routes en cache
Switch(config-if)#no ip mroute-cache	désactive l'enregistrement d routes en cache
Switch(config-if)#no ip directed-broadcast	désactive le broadcast dirigé
Switch(config-if)#no mop enabled	désactive le protocole de maintenance
Switch(config-if)#ntp disable	désactive le Network Time Protocol
Switch(config-if)#no cdp enable	pas de CISCO Discovery Protocol

* Le proxy ARP est un mécanisme permettant à un routeur de fournir son @MAC à la place de celle de la station demandée.

Exemple : *Un hôte d'un RSO-A a un masque lui permettant de joindre un hôte du RSO-B sans utiliser sa GW-A, alors le routeur fourni à la station du RSO-A son @MAC à la place de la station du RSO-B.*
Cela permet des routages non désirés.

Configurer une interface

```
Switch(config-if)#description texte
Switch(config-if)#speed 10, 100, auto
Switch(config-if)#duplex half, full, auto
```

NETTOYAGE DES INTERFACES

```
Switch(config-if)#no cdp enable                 pas de CISCO Discovery Protocol (facultatif)
Switch(config-if)#no snmp trap link-status      désactive les traps LINKDOWN/LINKUP
Switch(config-if)#no logging event link-status  désactive les logs LINKDOWN/LINKUP
Switch(config-if)#switchport nonegotiate        désactive le DTP (auto-trunking)
Switch(config-if)#no keepalive                  désactive les trames de LOOP
protocole de test CISCO d'état des interfaces ; à n'utiliser qu'avec des interfaces Ethernet
```

```
Switch(config-if)#shutdown
```
sur les switchs CISCO toutes les interfaces sont activées par défaut

VLAN - Assignation

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan num_vlan
```

VLAN - Trunking

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan num_vlan,num_vlan-num_vlan
Switch(config-if)#switchport trunk native vlan num_vlan     assigne les !TAG à un VLAN dédié
Switch(config-if)#switchport mode trunk
```

Mettre la sécurité sur les ports

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum nbre_@MAC_apprises
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown/restrict
```

Configurer un port en mode protégé

```
Switch(config-if)#switchport protected
```
Les stations d'un même VLAN et connectées aux ! protégés d'un même switch ne communiquent pas entre elles, mais avec celles connectées aux ! non protégés.
Contrairement au PVLAN, la notion de ! protégés n'existe pas entre les switchs, car c'est le ! qui est protégé et non le VLAN.

Créer un agrégat de lien

Créer l'aggrégat
Switch(config)#interface port-channel num_agg

Ajouter les interfaces à l'agrégat de liens
Switch(config)#interface fastethernet slot/port
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group num_agg mode active

Switch(config)#interface fastethernet slot/port
Switch(config-if)#channel-protocol lacp
Switch(config-if)#channel-group num_agg mode active

Entrer les paramètres communs aux interfaces membres de l'agrégat
Switch(config)#interface port-channel num_agg
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan ID,ID,ID
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotiate

Note: Les paramètres de l'agrégat de liens ne seront pas valables pour les interfaces ajoutées par la suite à l'agrégat