## Commandes IOS Cisco

## ***Convention d'écriture :***

italics indique des arguments dans lesquels l'utilisateur fournit des valeurs

[X] indique un élément facultatif

| indique un choix facultatif ou obligatoire

[X|Y] indique un choix facultatif

{X|Y} indique un choix obligatoire

## ***1 Commandes générales :***

## Commandes changement de mode d'exécution et de configuration :

R1> enable

R1# configure terminal

R1(config)#

R1(config)# exit | end | ^C | ^Z

R1# disable

R1>

## Appel de l’aide contextuelle :

**Entrer le caractère ?**

## Outils de diagnostic :

R1# ping *ip-address*

R1# traceroute *ip-address*

R1# show arp

## Visualisation de l'état de l'équipement :

R1# show version

R1# show flash

R1# show memory

R1# show interfaces

SW1# show history

SW1# terminal history size *{number*}

## Visualisation et sauvegarde de la configuration :

R1# show running-config

R1# show startup-config

R1# copy running-config startup-config

R1# copy running-config tftp:

SW1# copy system:running-config tftp:[[[//location]/directory]/filename]

SW1# copy nvram:startup-config tftp:[[[//location]/directory]/filename]

## Suppression du fichier de configuration :

R1# erase nvram:startup-config

R1# erase startup-config

## Configuration de base d'un équipement CISCO :

R1(config)# hostname *router-name*

R1(config)# enable password *password*

R1(config)# enable secret *password*

R1(config)# banner {motd | login} # *message* #

R1(config)# no ip domain-lookup

## Configuration de la console et du terminal virtuel :

R1(config)# line console 0

R1(config-line)# password *password*

R1(config-line)# login

R1(config-line)# logging synchronous

R1(config)# line vty 0 4

SW1(config)# line vty 0 15

R1(config-line)# password *password*

R1(config-line)# login

R1(config)# service password-encryption

## Récupération après la perte de mots de passe et d'IOS

## Sauvegarde et mise à niveau de l'image logicielle IOS :

R1# ping tftp-server-ip-address

R1# show flash:

R1# copy flash:old-ios tftp:

R1# copy tftp: flash:new-ios

R1(config)# boot system flash new-ios.bin

R1# copy running-config startup-config

R1# reload

## Récupération après la perte de mots de passe sur un routeur

1. Notez la valeur du registre avec la commande suivante :

R1> show version

2. Redémarrez le routeur. Lors du démarrage du routeur, il faut appuyer sur les touches Ctrl + Pause pour passer en mode ROM Monitor.

3. Entrez les commandes suivantes à fin de ne pas charger le fichier de configuration au démarrage du routeur.

rommon> confreg 0x2142

rommon> reset

4. Entrez les commandes suivantes pour réinitialiser un nouveau mot de passe et la valeur initiale du registre.

R1> enable

R1# copy startup-config running-config

R1# configure terminal

R1(config)# enable secret *password*

R1(config)# config-register 0x2102

R1(config)# end

R1# copy running-config startup-config

R1# reload

## Récupération d'IOS sur un routeur

Lors du démarrage du routeur, il faut appuyer sur les touches Ctrl + Pause pour passer en mode rommon.

rommon> IP\_ADDRESS=ip-address

rommon> IP\_SUBNET\_MASK=mask

rommon> DEFAULT\_GATEWAY=ip-address

rommon> TFTP\_SERVER=ip\_address

rommon> TFTP\_FILE=file\_name

rommon> tftpdnld

rommon> reset

## Récupération après la perte de mots de passe sur un commutateur

Pour récupérer le mot de passe sur un commutateur Cisco 2960, procédez comme suit :

1. Connectez un PC au port de la console du commutateur (9 600 bauds).

2. Redémarrez le commutateur, puis appuyez sur le bouton Mode pendant 15 secondes. Relâchez ensuite le bouton Mode.

3. Entrez les commandes suivantes :

SW1: flash\_init

SW1: load\_helper

SW1: rename flash:config.text flash:config.text.old

SW1: boot

4. Entrez les commandes suivantes :

SW1> enable

SW1# rename flash:config.text.old flash:config.text

SW1# copy flash:config.text system:running-config

SW1# configure terminal

SW1(config)# enable secret *password*

SW1# copy running-config startup-config

SW1# reload

## Récupération d'IOS sur un commutateur

1. Connectez un pc au port console du commutateur (9 600 bauds).

2. Entrez les commandes suivantes :

SW1:

SW1: set BAUD 115200

SW1: copy xmodem: flash:/ios.bin

ou

SW1: xmodem [-cyr] [ios.bin]

3. Configurez le logiciel pour une vitesse de ligne de 115200 bauds

4. Le commutateur se met en attente ; il est prêt à recevoir l'IOS par xmodem.

5. Cherchez le chier avec le menu du logiciel et envoyez-le par Xmodem.

6. Redémarrez :

SW1: reset

7. Après redémarrage, reconfigurez la vitesse de la ligne de console en 9600 bauds :

SW1(config)# line console 0

SW1(config-line)# speed 9600

## 2 Commutateurs

## Configuration de base d'un commutateur

## Configuration de l'interface de gestion sur un commutateur :

SW1(config)# interface vlan *vlan-id*

SW1(config-if)# ip address *ip-address subnet-mask*

SW1(config-if)# no shutdown

SW1(config)# ip default-gateway *ip-address*

SW1(config-if)# exit

## Configuration des interfaces

SW1(config)# interface *type port*

SW1(config)# interface range *type port {- | ,} port*

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan *vlan-id*

SW1# show ip interface brief

SW1# show ip interface

## Configuration d'options sur un port du commutateur :

SW1(config-if)# duplex {auto | full | half}

SW1(config-if)# speed {auto | *value-bps*}

SW1(config-if)# mdix auto

## Possibilité d'activer l'interface web pour la configuration du commutateur :

SW1(config)# ip http authentication enable

SW1(config)# ip http server

## Gestion de la table d'adresse MAC du commutateur :

SW1# show mac-address-table

SW1(config)# mac-address-table static *MAC-address* vlan {*1-4096* | ALL} interface *interface-id*

SW1(config)# mac-address-table static *MAC-address* vlan {*1-4096* | ALL} interface *interface-id* drop

SW1(config)# mac-address-table aging-time *secondes*

## Configuration de la sécurité sur les commutateurs.

## Configuration de la surveillance DHCP :

SW1(config)# ip dhcp snooping

SW1(config)# ip dhcp snooping vlan number [*number*]

SW1(config-if)# ip dhcp snooping trust

SW1(config-if)# ip dhcp snooping limit rate value

SW1# show ip dhcp snooping

## Configuration de la sécurité des ports :

SW1(config-if)# switchport port-security

SW1(config-if)# switchport port-security maximum number

SW1(config-if)# switchport port-security mac-address mac-address

SW1(config-if)# switchport port-security mac-address sticky [mac-address]

SW1(config-if)# switchport port-security violation {shutdown | restrict | protect}

SW1# show port-security [interface interface-id]

SW1# show port-security address

## Configuration du contrôle de tempête:

SW1(config-if)# storm-control {{broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}} | {action {shutdown | trap}}

## Désactivation du mode DTP:

SW1(config-if)# switchport nonegociate

## Activation du port miroring (SPAN et RSPAN)

## SPAN:

SW1(config)# monitor session *number* source interface *interface interface-id*

SW1(config)# monitor session *number* destination interface *interface interface-id* encapsulation replicate

## RSPAN:

SW1(config)# monitor session *number* source interface *interface interface-id*

SW1(config)# monitor session *number* destination remote vlan *vlan-id* reflector-port *interface interface-id* SW2(config)# monitor session *number* source remote vlan *vlan-id*

SW2(config)# monitor session *number* destination interface *interface interface-id*

## Réseaux locaux virtuels VLANs

## Configuration de VLANs :

SW1(config)# vlan vlan-id

SW1(config-vlan)# name vlan-name

SW1# show vlan [brief | id vlan-id | name vlan-name | summary]

SW1# show interfaces [interface-id | vlan vlan-id] | switchport

SW1# delete flash:vlan.dat

## Configuration de base de VLANs avec VLAN VoIP :

SW1(config)# interface type port

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan vlan-id

SW1(config-if)# mls qos trust cos

SW1(config-if)# switchport voice vlan voice-vlan-id

## Configuration d'agrégations de VLANs (Trunk) :

SW1(config)# interface type port

SW1(config-if)# switchport mode trunk

SW1(config-if)# switchport trunk native vlan vlan-id

SW1(config-if)# switchport trunk allowed vlan vlan-id [,vlan-id,vlan-id ...]

SW1(config-if)# switchport trunk allowed vlan add vlan-id

SW1# show interfaces id-interface SW1port

SW1# show interfaces trunk

## Dynamic Trunking Protocol DTP :

SW1(config)# interface type port

SW1(config-if)# switchport mode access

SW1(config-if)# switchport mode trunk

SW1(config-if)# switchport mode dynamic auto

SW1(config-if)# switchport mode dynamic desirable

SW1(config-if)# switchport nonegociate

SW1# show dtp interface type port

## VLAN Trunking Protocol VTP

## Configuration de VTP :

SW1(config)# vtp mode {server | client | transparent}

SW1(config)# vtp domain domain-name

SW1(config)# vtp password password

SW1(config)# vtp version {1 | 2}

SW1(config)# vtp pruning

SW1# show vtp status

SW1# show vtp counters

SW1# show interfaces trunk

## Spanning Tree Protocol STP

## Configuration de la sélection du pont racine et des ports racines, désignés et non-désignés :

SW1(config)# spanning-tree vlan vlan-id root primary

SW1(config)# spanning-tree vlan vlan-id root secondary

SW1(config)# spanning-tree vlan vlan-id priority value

SW1(config-if)# spanning-tree cost value

SW1(config-if)# spanning-tree port-priority value

SW1# show spanning-tree [detail | active]

## Configuration de quelques paramètres de SPT :

SW1(config)# spanning-tree vlan vlan-id root primary diameter value

## Sécurisation de SPT :

SW1(config-if)# spanning-tree portfast

SW1(config-if)# spanning-tree portfast default

SW1(config-if)# spanning-tree portfast bpduguard default

SW1(config-if)# spanning-tree guard root

## Configuration de Rapid-PVST+ :

SW1(config)# spanning-tree mode rapid-pvst

SW1(config)# interface type port

SW1(config-if)# spanning-tree link-type point-to-point

SW1(config-if)# end

SW1# clear spanning-tree detected-protocols

## Etherchannel

SW1(config)# interface range type port - port

SW1(config-if)# switchport mode {access | trunk}

SW1(config-if)# [switchport access vlan *vlan-id | trunk allowed vlan vlan-id]*

SW1(config-if)# channel-group etherchannel-id mode [auto | desirable| on | active | passive | on]

SW1(configf)# port-channel load-balance [dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac]

## ***3 Routage inter-vlan***

## Configuration de sous-interfaces sur un R1-on-a-stick :

R1(config)# interface type interface-number

R1(config-if)# no shutdown

R1(config-if)# interface type interface-number.subinterface-number

R1(config-subif)# encapsulation dot1q vlan-id [native]

R1(config-subif)# ip address ip-address subnet-mask

R1#show vlans

## Commutation de niveau 3:

SW1[config]# ip routing

## Creation de SVI

SW1(config)# interface type port

SW1(config)# interface vlan *vlan-id*

SW1(config-if)# ip address *ip-address subnet-mask*

## Creation de port routed (equivalent interface routeur)

SW1(config)# interface type port

SW1(config-if)# no switchport

SW1(config-if)# ip address *ip-address subnet-mask*

SW1(config)# ip route 0.0.0.0 0.0.0.0 [*ip-gateway | interface-type/port*]

## Activation commutation de niveau 3 sur 2960:

SW1# show sdm prefer

SW1(config)# sdm prefer {default | dual-ipv4-and-ipv6 |lanbase-routing | qos]

SW1# reload

## Port routed remplacé par Routes statiques sur 2960

SW1(config)# ip route *network interface-type/port*

## 4 Routeurs

## Configuration de base d'un routeur

## Configuration des interfaces sur un routeur :

R1(config)# interface type port

R1(config-if)# ip address ip-address subnet-mask

R1(config-if)# description description

R1(config-if)# clock rate rate

R1(config-if)# no shutdown

R1(config-if)# exit

R1# show ip interface brief

R1# show ip interface

## Configuration de IPv6 :

R1X(config)# ipv6 unicast-routing

R1X(config-if)# ipv6 address ipv6-address /prefix-length [eui-64]

R1X(config)# ipv6 host name [port] ipv6addr [ipv6addr ...]

R1X(config)# ip name-server address

## Visualisation et dépannage pour le routage, valable pour tous les protocoles de routage :

R1# ping ip-address

R1# traceroute ip-address

R1# show ip route

R1# show ip interface brief

R1# show running-config

R1# show cdp neighbors detail

R1# debug ip routing

R1# undebug ip routing

R1# undebug all

## Visualisation et dépannage d'IPv6 :

R1X# show ipv6 interface

R1X# show ipv6 interface brief

R1X# show ipv6 neighbors

R1X# show ipv6 protocols

R1X# show ipv6 rip

R1X# show ipv6 route

R1X# show ipv6 route summary

R1X# show ipv6 routers

R1X# show ipv6 static

R1X# show ipv6 static interface interface

R1X# show ipv6 static detail

R1X# show ipv6 traffic

R1X# clear ipv6 rip

R1X# clear ipv6 route \*

R1X# clear ipv6 traffic

R1X# debug ipv6 packet

R1X# debug ipv6 rip

R1X# debug ipv6 routing

## Installation du package technique de sécurité

R1(config)# license boot module c1900 technology-package securityk9

## Cisco SDM

## Configuration du routeur pour la prise en charge de SDM :

R1# configure terminal

R1(config)# ip http server

R1(config)# ip http secure-server

R1(config)# ip http authentication local

R1(config)# username name privilege 15 secret password

R1(config)# line vty 0 4

R1(config-line)# privilege level 15

R1(config-line)# login local

R1(config-line)# transport input telnet ssh

R1(config-line)# exit

## Cisco Discovery Protocol (CDP) :

R1# show cdp neighbors

R1# show cdp neighbors detail

R1(config)# no cdp run

R1(config-if)# no cdp enable

## Routage statique

## Configuration de routes statiques et route statique par défaut :

R1(config)# ip route prefix mask {ip-address | interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]

R1(config)# ip route network-address subnet-mask {ip-address |exit-interface}

R1(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]

## Routage dynamique

## RIPv1,RIPv2 et RIPng

Configuration de RIPv1 :

R1(config)# router rip

R1(config-router)# version 1

R1(config-router)# network directly-connected-classful-address

R1(config-router)# passive-interface interface-type interface-number

## Configuration de RIPv2 :

R1(config)# router rip

R1(config-router)# version 2

R1(config-router)# network directly-connected-classful-address

R1(config-router)# passive-interface interface-type interface-number

R1(config-router)# no auto-summary

## Redistribution de route statique et propagation de la route par défaut :

R1(config-router)# redistribute static

R1(config-router)# default-information originate

## Dépannage de RIP :

R1# show ip route

R1# show ip rip database

R1# show ip protocols

R1# debug ip rip

## Comportement du routage par classe et sans classe :

R1(confi)# ip classless

R1(confi)# no ip classless

## Configuration de RIPv2 avec authentification du protocole de routage :

R1(config)# router rip

R1(config-router)# passive-interface default

R1(config-router)# no passive-interface interface-type interface-number

R1(config)# key chain RIP\_KEY

R1(config-keychain)# key 1

R1(config-keychain-key)# key-string string

R1(config)# interface type port

R1(config-if)# ip rip authentification mode md5

R1(config-if)# ip rip authentification key-chain RIP\_KEY

R1# show ip route

## Configuration de RIPng :

R1(config)# ipv6 unicast-routing

R1(config)# ipv6 router rip *domain-name*

R1(config-if)# ipv6 rip *domain-name* enable

R1(config-if)# ipv6 rip *domain-name* default-information originate

R1# show ipv6 protocols

R1# show ipv6 route

## EIGRP

## Configuration d'EIGRP :

R1(config)# router eigrp autonomous-system

R1(config-router)# network network-address [wildcard-mask]

R1(config-router)# passive-interface interface-type interface-number

R1(config-router)# no auto-summary

## Propagation de la route par défaut et résumé de réseaux :

R1(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]

R1(config-router)# redistribute static

R1(config)# ip default-network network-address

R1(config-if)# ip summary-address eigrp as-number network-address subnet-mask

## Configuration de bande passante et autres caractéristiques pour le calcul de la métrique d'EIGRP:

R1(config-router)# metric weights tos k1 k2 k3 k4 k5

R1(config-if)# bandwidth bw-kbps

R1(config-if)# ip bandwidth-percent eigrp as-number percent

R1# show interface interface-type interface-number

R1(config-if)# ip hello-interval eigrp as-number seconds

R1(config-if)# ip hold-time eigrp as-number seconds

## Visualisation et dépannage d'EIGRP :

R1# show ip eigrp neighbors

R1# show ip eigrp topology [network | all-links]

R1# show ip route

R1# show ip interface brief

R1# show interface interface-type interface-number

R1# show ip protocols

R1# debug eigrp fsm

## Configuration d'EIGRP avec authentification du protocole de routage :

R1(config)# key chain EIGRP\_KEY

R1(config-keychain)# key 1

R1(config-keychain-key)# key-string string

R1(config)# interface type port

R1(config-if)# ip authentification mode eigrp as md5

R1(config-if)# ip authentification key-chain eigrp as EIGRP\_KEY

R1 # show ip route

## OSPF

## Configuration d'OSPFv2 :

R1(config)# router ospf process-id

R1(config-router)# network network-address wildcard-mask area area-id

R1(config-router)# passive-interface interface-type interface-number

## Configuration de l'ID du routeur en configurant une interface de bouclage (Loopback) ou avec la commande router-id :

R1(config-router)# routeur-id ip-address

R1(config-if)#ip ospf priority {0 255}

R1(config)#interface loopback number

R1(config-if)#ip address ip-address subnet-mask

R1#clear ip ospf process

## Configuration de la bande passante ou du coût pour le calcul de la métrique d'OSPF :

R1(config-router)# auto-cost reference-bandwidth value-mbps

R1(config-if)# bandwidth bw-kbps

R1(config-if)# ip ospf cost cost

R1# show interface interface-type interface-number

R1(config-if)# ip ospf hello-interval seconds

R1(config-if)# ip ospf dead-interval seconds

## Propagation de la route par défaut :

R1(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]

R1(config-router)# default-information originate

## Visualisation et dépannage d'OSPFv2 :

R1# show ip route

R1# show ip interface brief

R1# show ip ospf [interface interface-type interface-number]

R1# show ip ospf neighbor

R1# show interface interface-type interface-number

R1# show ip protocols

## Configuration d'OSPF avec authentification simple du protocole de routage :

R1(config)# router ospf process-id

R1(config-router)# area area-id authentification

R1(config)# interface type port

R1(config-if)# ip ospf authentication

R1(config-if)# ip ospf authentication-key string

R1# show ip route

## Configuration d'OSPF avec authentification md5 du protocole de routage :

R1(config)# interface type port

R1(config-if)# ip ospf message-digest-key 1 md5 string

R1(config-if)# ip ospf authentication message-digest

R1(config)# router ospf process-id

R1(config-router)# area area-id authentication message-digest

R1# show ip route

## Configuration d'OSPFv3 :

1. Valider le routage unicast IPv6

R1(config)# ipv6 unicast-routing

2. Configurer les adresses de lien local IPv6 (optionnel, identification routeur plus simple)

R1(config-if)# ipv6 adress *fe80::1* link-local

3. configurer un ID de process OSPFv3

R1(config)# ipv6 router ospf *process-id*

4. configurer un ID de routeur

R1(config-rtr)# router-id *ip-address*

5. Activer OSPFv3 sur les interfaces

R1(config-if)# ipv6 ospf *process-id* area *area-id*

6. configurer les options spécifiques de routage

R1(config-rtr)# auto-cost reference-bandwidth *value-mbps*

R1(config-rtr)# passive-interface *interface-type interface-number*

R1(config-if)# bandwidth *bw-kbps*

## Visualisation et dépannage d'OSPFv3 :

R1# show ipv6 protocols

R1# clear ipv6 ospf process

R1# show ipv6 ospf interface

R1# show ipv6 ospf interface *interface-type interface-number*

R1# show ipv6 ospf interface brief

R1# show ipv6 ospf neighbor

R1# show ipv6 ospf

R1# show ipv6 ospf interface brief

R1# show ipv6 ospf interface *interface-type interface-number*

R1# show ipv6 route ospf

## ***Sécurisation générale du routeur***

## Processus de sécurisation automatique du routeur :

R1# auto secure

R1(config)# Secure boot-image

R1(config)# Secure boot-config

R1# show secure bootset

**R1(config)# secure boot-config restore nom-image-config**

## Privilèges d’accès au routeur :

R1(config)# privilege [mode] {level [niveau de privilege] | reset} [liste des commandes autorisées]

R1(config)# username *username* privilege *level* secret *password*

## Privilèges d’accès par View au routeur :

R1(config)# aaa new-model]

## Root view

R1(config)# enable view

## CLI view

R1(config)# parser view showview

R1(config-view)# secret *password*

R1(config-view)# commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command]

## Superview

R1(config)# parser view *user* superview

R1(config-view)# secret *password*

R1(config-view)# view showview

## Accès par privilège

R1> enable view *user*

## Configuration de mots de passe sécurisés et authentification AAA :

R1(config)# aaa new-model

R1(config)# aaa authentication login LOCAL\_AUTH local

R1(config)# line console 0

R1(config-line)# login authentication LOCAL\_AUTH

R1(config-line)# line vty 0 4

R1(config-line)# login authentication LOCAL\_AUTH

R1# username username password password

R1# username username secret password

R1(config)# service password-encryption

R1(config)# security passwords min-length number

## Configuration RADIUS - TACACS+:

R1(config)# aaa authentication login [default nom\_liste\_methode] [radius | tacacs+]

R1(config)# aaa authorization {network | exec | commands level} {default | list-name} method1...[method4] l

R1(config)# aaa authentication login default group tacacs+

R1(config)# aaa authorization exec default group tacacs+

R1(config)# aaa authorization network default group tacacs+

R1(config)# aaa accounting exec default start-stop group tacacs+

R1(config)# aaa accounting network default start-stop group tacacs+

## Désactivation de la ligne auxiliaire :

R1(config)# line aux 0

R1(config-line)# no password

R1(config-line)# login

R1(config-line)# exit

## Configuration des lignes de terminaux virtuels VTY pour Telnet et SSH :

R1(config)# line vty 0 4

R1(config-line)# no transport input

R1(config-line)# transport input telnet ssh

R1(config-line)# exit

R1(config)# login block-for seconds attempt tries within seconds

R1(config)# login delay 5

R1(config)# login quiet-mode access-class {acl-name | acl-number}

R1(config)# security authentication failure rate threshold-rate log

## Configuration des lignes de terminaux virtuels VTY uniquement pour SSH :

R1(config)# line vty 0 4

R1(config-line)# no transport input

R1(config-line)# transport input ssh

R1(config-line)# exec-timeout number

R1(config)# service tcp-keepalives-in

## Configuration de SSH :

R1(config)# ip ssh version 2

R1(config)# hostname hostname

R1(config)# ip domain-name domain-name

R1(config)# crypto key {generate | zeroise} rsa

R1(config)# username username secret password

R1(config)# line vty 0 4

R1(config-line)# transport input ssh

R1(config-line)# login local

R1(config)# ip ssh time-out seconds

R1(config)# ip ssh authentification-retries number

R1# show ip ssh

R1# show ssh

## Désactivation des services non utilisés :

R1# show running-config

R1(config)# no service tcp-small-servers

R1(config)# no service udp-small-servers

R1(config)# no ip bootp server

R1(config)# no service finger

R1(config)# no ip http server

R1(config)# no snmp-server

R1(config)# no cdp run

R1(config)# no service config

R1(config)# no ip source-route

R1(config)# no ip classless

R1(config-if)# shutdown

R1(config-if)# no ip directed-broadcast

R1(config-if)# no ip proxy-arp

## 5 Liste de Contrôle d'Accès ACL

## ACL standard IPv4

## Configuration d'une ACL standard numérotée:

R1(config)# access-list access-list-number {permit | deny | remark remark} source [source-wildcard] [log]

R1(config)# no access-list acces-list-number

R1(config-if)# ip access-group {access-list-number | access-list-name} {in | out}

R1# show access-lists [acces-list-number | NAME]

## Configuration d'une ACL standard nommée :

R1(config)# ip access-list standard NAME

R1(config-std-nacl)# sequence-number [permit | deny | remark] source [source-wildcard] [log]

R1(config-if)# ip access-group access-list-name {in | out}

R1# show access-lists [NAME]

## Utilisation d'une ACL pour contrôler l'accès aux lignes virtuelles VTY :

R1(config)# access-list access-list-number {deny | permit} source [source-wildcard]

R1(config)# line vty 0 4

R1(config-line)# access-class access-list-number in [vrf-also] | out

## ACL étendue IPv4

## Configuration d'une ACL étendue numérotée:

R1(config)# access-list access-list-number {permit | deny | remark}

protocol source [source-wildcard] [operator operand] [port port-number or name] destination [destination-wildcard [operator operand] [port port-number or name] [established]

R1(config)# access-list access-list-number {permit | deny} protocol source source-wildcard destination destination-wildcard {eq | neq | gt | lt | range} protocol-number [established]

R1(config-if)# ip access-group {access-list-number | access-list-name}{in | out}

R1# show access-lists [acces-list-number | NAME]

## Configuration d'une ACL étendue nommée :

R1(config)# ip access-list extended NAME

R1(config-ext-nacl)# sequence-number [permit | deny | remark] protocol source [source-wildcard] destination [destination-wildcard] {eq | neq | gt | lt | range} protocol-number [established]

R1(config-if)# ip access-group access-list-name {in | out}

R1# show access-lists [NAME]

## ACL dynamique IPv4

## Exemple de configuration d'une ACL dynamique :

R1(config)# username name password password

R1(config)# access-list access-list-number dynamic dynamic-name [timeout minutes] permit telnet source source-wildcard destination destination-wildcard

R1(config-if)# ip access-group access-list-number in

R1(config)# line vty 0 4

R1(config-line)# autocommand access-enable host timeout minutes

## ACL réflexive IPv4

## Exemple de configuration d'une ACL réflexive :

R1(config)# ip access-list extended OUT-NAME

R1(config-ext-nacl)# permit protocol source source-wildcard destination destination-wildcard reflect reflect-NAME

R1(config)# ip access-list extended IN-NAME

R1(config-ext-nacl)# evaluate reflect-NAME

R1(config-if)# ip access-group IN-NAME in

R1(config-if)# ip access-group OUT-NAME out

## ACL basée sur le temps IPv4

## Exemple de configuration d'une ACL basée sur le temps :

R1(config)# time-range NAME

R1(config-time-range)# periodic DAYS hh:mm to hh:mm

R1(config)# access-list ACL-number permit protocol [source-ipv6-prefix/prefix-length | any | host source-ipv6-address] [operator [port-number]] destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address] [operator [port-number]]

R1(config-if)# ip access-group ACL-number {in | out}

## Viisualisation et dépannage des ACLs IPv4 :

R1(config)# show access-lists

## ACLs IPv6 nommée

R1(config)# ipv6 access-list *access-list-name*

R1(config-ipv6-acl)# [permit | deny | remark] protocol source [source-wildcard] destination [destination-wildcard] {eq | neq | gt | lt | range} protocol-number [established]

R1(config-if)# ipv6 traffic-filter *access-list-name* {in | out}

## Viisualisation et dépannage des ACLs IPv6 :

R1(config)# show ipv6 interface

R1(config)# show access-lists [acces-list-number | NAME]

R1(config)# show running-config

## 6 NAT et PAT

## Configuration de la NAT statique :

R1(config)# ip nat inside source static local-ip global-ip

R1(config)# interface type number

R1(config-if)# ip nat inside

R1(config)# interface type number

R1(config-if)# ip nat outside

## Configuration de la redirection de port :

R1(config)# ip nat inside source static protocol local-ip port global-ip port

## Configuration de la NAT dynamique :

R1(config)# ip nat pool NAME start-ip end-ip {netmask netmask | prefix-length prefix-length}

R1(config)# access-list access-list-number permit source [source-wildcard]

R1(config)# ip nat inside source list access-list-number pool NAME

R1(config)# interface type number

R1(config-if)# ip nat inside

R1(config)# interface type number

R1(config-if)# ip nat outside

## Configuration de la surcharge NAT première configuration possible :

R1(config)# access-list access-list-number permit source [source-wildcard]

R1(config)# ip nat inside source list access-list-number interface interface overload

R1(config)# interface type number

R1(config-if)# ip nat inside

R1(config)# interface type number

R1(config-if)# ip nat outside

## Configuration de la surcharge NAT deuxième configuration possible :

R1(config)# access-list access-list-number permit source [source-wildcard]

R1(config)# ip nat pool NAME start-ip end-ip {netmask netmask | prefix-length prefix length}

R1(config)# ip nat inside source list access-list-number pool NAME overload

R1(config)# interface type number

R1(config-if)# ip nat inside

R1(config)# interface type number

R1(config-if)# ip nat outside

## Visualisation et dépannage de NAT :

R1# show ip nat translations [verbose]

R1# show ip nat statistics

R1# clear ip nat statistics

R1(config)# ip nat translation timeout timeout-seconds

R1# clear ip nat translation \*

R1# clear ip nat translation inside global-ip local-ip [outside local-ip global-ip]

R1# clear ip nat translation protocol inside global-ip global-port local-ip local-port [outside local-ip local-port global-ip global-port]

R1# debug ip nat [detailed]

## 7 FIREWALL

## Firewall CBAC

## 1°) Choix des interfaces internes et externes pour l’application des règles d’inspection.:

***2°) Configuration des ACL sur les interfaces :***

***3°) Définir la règle d’inspection :***

R1(config)# ip inspect name inspection\_name protocol [alert {on | off}] [audit-trail {on | off}] [timeout seconds]

***4°) Appliquer la règle d’inspection à l’interface qui initie le trafic dans le sens IN.***

R1(config)# interface interface-type interface-number

R1(config)# ip inspect inspection\_name {in | out}

## Firewall ZBF

## 1°) Determination des Zones :

R1(config)# zone security zone-name

R1(config-sec-zone)# description line-of-description

***2°) Définir les classes de trafic :***

R1(config)# class-map type inspect [match-any | match-all] class-map-name

R1(config)# class-map type inspect protocol-name [match-any | match-all] class-map-name

R1(config-cmap)# match access-group {access-group | name access-group-name}

R1(config-cmap)# match protocol protocol-name

R1(config-cmap)# match class-map class-map-name

***3°) Définir les polices du pare-feu :***

R1(config)# policy-map type inspect policy-map-name

R1(config-pmap)# class type inspect class-name

R1(config-pmap-c)# pass | inspect | drop [log] | police

***4°) Appliquer les polices aux zones appariées.***

R1(config)# zone-pair security zone-pair-name [source source-zone-name | self] destination [self | destination-zone-name]

R1(config-sec-zone-pair)# service-policy type inspect policy-map-name

***5°) Assigner les interfaces aux zones.***

R1(config-if)# zone-member security zone-name

## 8 IDS-IPS

## IOS IPS5.x de Cisco

## 1°) Téléchargez les 2 fichiers IOS IPS suivants sur un serveur FTP:

IOS-Sxxx-CLI.pkg – le dernier package de signatures.

realm-cisco.pub.key.txt – La clé de chiffrement publique utilisé par IOS IPS.

***2°) Créer dans la flash un répertoire de configuration IOS IPS:***

R1#mkdir ips

***3°) Configurer une clé de chiffrement IOS IPS :***

Collez-le fichier texte realm-cisco.pub.key.txtdans la console en mode de configuration globale

***4°) Activer IPS IOS: Définir le nom des règles IPS et sa localisation.***

R1(config)# ip ips name iosips

R1(config)# ip ips config location flash:ips

***5°) Valider les notifications SDEE ou/et Syslog***

R1(config)# ip http server

R1(config)# ip ips notify [log | sdee]

***6°) Configurer la catégorie des signatures.***

R1(config)# ip ips *signature-category*

***7°) Sélectionner les catégories de signature à utiliser.***

R1(config-ips-category)# retired true

R1(config-ips-category)# category *category* [all, basic, advanced]

R1(config-ips-category)# retired false

***8°) Modifier éventuellement l’action associée à une signature***

R1(config-ips-category-action)# event-action [produce-alert | deny-packet-inline | reset-tcp-connection]

***9°) Appliquer la règle IPS sur l’interface et définir la direction de l’analyse***

R1(config)# interface interface-type interface-number

R1(config-if)# ip ips iosips in

***10°) Chargez le package de signature IOS IPS dans le routeur.***

R1# copy ftp://ftp\_user:password@Server\_IP\_address/ IOS-Sxxx-CLI.pkg idconf

## 9 Réseaux privés virtuels VPN

## Configuration d'un VPN GRE, à configurer sur les routeurs de chaque site:

R1(config)# interface tunnel 0

R1(config-if)# ip address *ip-address subnet-mask*

R1(config-if)# tunnel source *wan-source-interface*

R1(config-if)# tunnel destination *wan-destination-interface-IP*

R1(config-if)# tunnel mode gre ip

## Configuration d'un VPN IPsec site à site, à configurer sur les routeurs de chaque site:

## 1°) configuration des ACL compatibles avec IPsec (permit AH, ESP, ISAKMP):

R1(config)# access-list 101 permit ahp source dest

R1(config)# access-list 101 permit esp source dest

R1(config)# access-list 101 permit udp source dest eq isakmp

R1(config)# interface interface-type interface-number

R1(config-if)# ip access-group in

***2°) configuration d’IKE:***

R1(config)# crypto isakmp policy *priority*

R1(config-isakmp)# authentification [preshare | rsa-encr | rsa-sig]

R1(config-isakmp)# encryption [des | 3des | aes | aes 192 | aes 256]

R1(config-isakmp)# group [1 | 2 | 3]

R1(config-isakmp)# hash [sha | md5]

R1(config-isakmp)# lifetime *seconds*

***configuration d’IKE avec PSK (uniquement si pre-share choisi)***

R1(config)# crypto isakmp key keystring address peer-address

R1(config)# crypto isakmp key keystring hostname hostname

***3°) configuration des transform sets:***

R1(config)# crypto ipsec transform-set *transform-set-name* [ah-md5-hmac | …| comp-lzs]

***4°) configuration de la crypto ACL.***

R1(config)# access-list *crypto-acl-number* permit source-LAN dest-LAN

***5°) configuration et application de la crypto map.***

R1(config)# crypto map *map-name* *seq-num* [ipsec-manual | ipsec-isakmp [dynamic [dynamic-map-name]]]

R1(config-crypto-map)# match address *crypto-acl-number*

R1(config-crypto-map)#set peer *wan-IP-adress* [default]

R1(config-crypto-map)# set peer secondary-*wan-IP-adress*

R1(config-crypto-map)#set pfs [group1 | group2]

R1(config-crypto-map)#set transform-set *transform-set-name*

R1(config-crypto-map)#set security-association lifetime seconds 86400

R1(config)# interface interface-type interface-number

R1(config-if)# crypto map *map-name*

***6°) visualisation et dépannage IPsec.***

R1(config)# show crypto map

R1(config)# show crypto isakmp policy

R1(config)# show crypto ipsec sa

R1(config)# show crypto ipsec transform-set

R1(config)# debug crypto isakmp

R1(config)# debug crypto ipsec

## Configuration d'un VPN entre un site et un client :

R1(config)# username name password password

R1(config)# vpdn enable

R1(config-vpdn)# accept-dialin

R1(config-vpdn-acc-in)# protocol pptp

R1(config-vpdn-acc-in)# virtual-template 1

R1(config-vpdn-acc-in)# interface virtual-template 1

R1(config-if)# ip unnumbered local-interface

R1(config-if)# peer default ip address pool POOL\_NAME

R1(config-if)# ppp authentication {ms-chap | chap | pap}

R1(config)# ip local pool POOL\_NAME low-address high-address

## 10 Consignation SNMP - Syslog

## Configuration de la consignation via le protocole SNMP vers le serveur Syslog :

R1(config)# logging syslog-server-ip-address

R1(config)# logging trap {emergencies | alerts | critical | errors | warnings| notifications | informational | debugging}

R1(config)# logging source-interface loopback 0

R1(config)# login on

R1(config)# login buffered on

R1(config)# login on-success log [every login]

R1(config)# login on-failure log [every login]

## 11 Serveur NTP

## Configuration d’un serveur NTP :

R1# clock set 10:28:00 8 may 2010

R1#update-calendar

R1(config)# ntp master 1

R1(config)# ntp authenticate

R1(config)# ntp authentication-key 1 md5 cisco

R1(config)# ntp trusted-key 1

## Configuration d’un client NTP :

R1(config)# ntp server *IP-adress*

R1(config)# ntp authenticate

R1(config)# ntp authentication-key 1 md5 cisco

R1(config)# ntp trusted-key 1

R1(config)# ntp update-calendar

## 12 Protocole DHCP

## Configuration d'un serveur DHCP IPv4:

R1(config)# service dhcp

R1(config)# ip dhcp excluded-address low-address [high-address]

R1(config)# ip dhcp pool pool-name

R1(dhcp-config)# network network-number [mask | /prefix-length]

R1(dhcp-config)# default-router address [address2 ...address8]

R1(dhcp-config)# dns-server address [address2 ...address8]

R1(dhcp-config)# domain-name domain

R1(dhcp-config)# lease {days [hours] [minutes] | infinite}

R1(dhcp-config)# netbios-name-server address [address2 ...address8]

## Configuration d'un relais DHCP IPv4:

R1(config-if)# ip helper-address server-address

R1# show ip interface interface-type interface-number

## Visualisation et dépannage de DHCP IPv4:

R1# show ip dhcp binding

R1# show ip dhcp server statistics

R1# show ip dhcp server pool

R1# show ip dhcp conflict

R1# debug ip dhcp server events

R1# debug ip packet

## Configuration d'un serveur Stateless DHCPv6:

R1(config)# ipv6 unicast-routing

R1(config)# ipv6 dhcp pool pool-name

R1(config-dhcpv6)# dns-server address [address2 ...address8]

R1(config-dhcpv6)# domain-name domain

R1(config)# interface interface-type interface-number

R1(config-if)# ipv6 dhcp server pool-name

R1(config-if)# ipv6 nd other-config-flag

## Configuration d'un client Stateless DHCPv6:

R1(config)# interface interface-type interface-number

R1(config-if)# ipv6 enable

R1(config-if)# ipv6 address autoconfig

## Configuration d'un serveur Stateful DHCPv6:

R1(config)# ipv6 unicast-routing

R1(config)# ipv6 dhcp pool pool-name

R1(config-dhcpv6)# address prefix/length [lifetime *valid-lifetime preferred-lifetime* | infinite]

R1(config-dhcpv6)# dns-server address [address2 ...address8]

R1(config-dhcpv6)# domain-name domain

R1(config)# interface interface-type interface-number

R1(config-if)# ipv6 dhcp server pool-name

R1(config-if)# ipv6 nd managed-config-flag

## Configuration d'un client Stateful DHCPv6:

R1(config)# interface interface-type interface-number

R1(config-if)# ipv6 enable

R1(config-if)# ipv6 address dhcp

## Configuration d'un relais DHCPv6:

R1(config-if)# ipv6 dhcp relay destination server-address

## Visualisation et dépannage de DHCPv6:

R1# show ipv6 dhcp pool

R1# debug ipv6 dhcp binding

R1# debug ipv6 dhcp detail

R1# show ipv6 interface

R1# show ipv6 interface interface-type interface-number

R1# show ipv6 dhcp conflict

## 13 Réseaux étendus WAN

## Point-to-Point Protocol PPP

## Activation du protocole hdlc sur une interface série :

R1(config-if)# encapsulation hdlc

## Activation du protocole ppp sur une interface série :

R1(config-if)# encapsulation ppp

R1(config-if)# compress [predictor | stac]

R1(config-if)# ppp quality percentage

## Fonction de rappel PPP :

R1(config-if)# ppp callback [accept | request]

## Protocole d'authentification du mot de pass PAP et CHAP :

R1(config-if)# ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default] [callin]

R1(config)# username name password password

R1(config-if)# ppp pap sent-username name password password

## Exemple de configuration de PAP entre deux routeurs R1 et R2 :

R1(config)# username User2 password User2-password

R1(config-if)# encapsulation ppp

R1(config-if)# ppp authentication pap

R1(config-if)# ppp pap sent-username User1 password User1-password

R2(config)# username User1 password User1-password

R2(config-if)# encapsulation ppp

R2(config-if)# ppp authentication pap

R2(config-if)# ppp pap sent-username User2 password User2-password

## Même exemple mais en utilisant CHAP :

R1(config)# username User2 password User2-password

R1(config-if)# encapsulation ppp

R1(config-if)# ppp authentication chap

R1(config-if)# ppp chap hostname User1

R1(config-if)# ppp chap password User1-password

R2(config)# username User1 password User1-password

R2(config-if)# encapsulation ppp

R2(config-if)# ppp authentication chap

R2(config-if)# ppp chap hostname User2

R2(config-if)# ppp chap password User2-password

## Visualisation et dépannage d'une interface série :

R1# show interfaces serial interface-number

R1# show controllers

R1# debug ppp {packet | negotiation | error | authentification | compression | cbcp}

## Frame Relay

## Configuration de Frame Relay avec mappage statique :

R1(config-if)# encapsulation frame-relay [cisco | ietf]

R1(config-if)# bandwidth bw-kbps

R1(config-if)# no frame-relay inverse-arp

R1(config-if)# frame-relay map protocol protocol-address dlci [broadcast] [ietf] [cisco]

R1# show frame-relay map

## Interface de supervision locale LMI :

R1# show frame-relay lmi

R1# frame-relay lmi-type [cisco | ansi | q933a]

## Configuration de sous-interfaces Frame Relay :

R1(config)# interface serial interface

R1(config-if)# encapsulation frame-relay

R1(config-if)# interface serial subinterface\_number [multipoint |point-to-point]

R1(config-subif)# ip address ip-address subnet-mask

R1(config-subif)# frame-relay interface-dlci dlci-number

R1(config-if)# no shutdown

## Visualisation et dépannage de Frame Relay :

R1# show interfaces

R1# show frame-relay lmi

R1# show frame-relay pvc [interface interface] [dlci]

R1 # clear counters

R1 # show frame-relay map

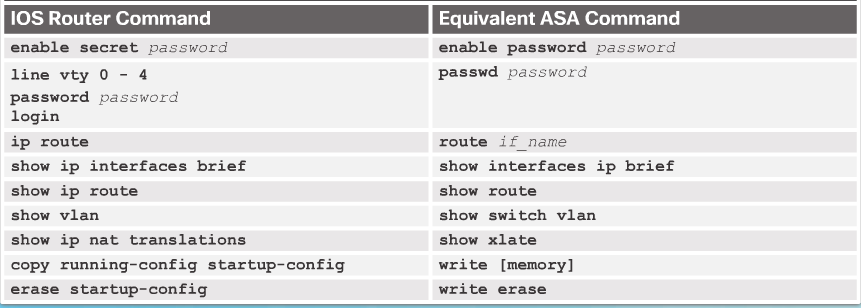
R1 # clear frame-relay-inarp

R1 # debug frame-relay lmi

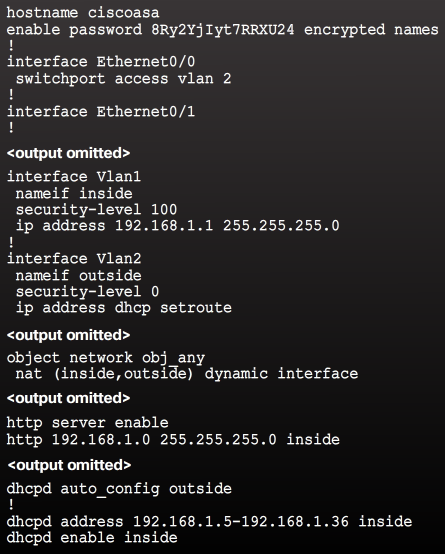
**Commandes CLI ASA**

**Basic ASA Settings**

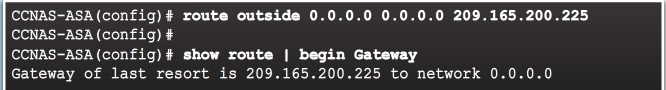
Pour beaucoup de commande, identique à la syntaxe ios cisco



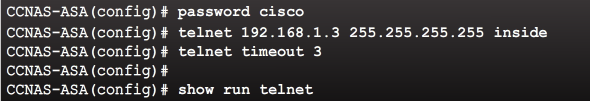
Configuration de base



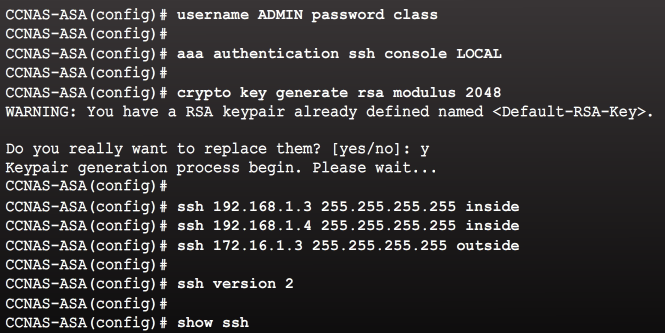
Configuration route par defaut



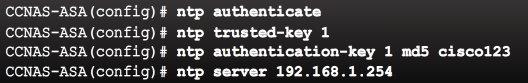
Configuration telnet



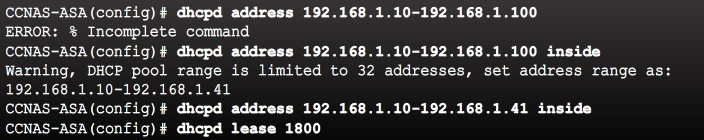
Configuration ssh



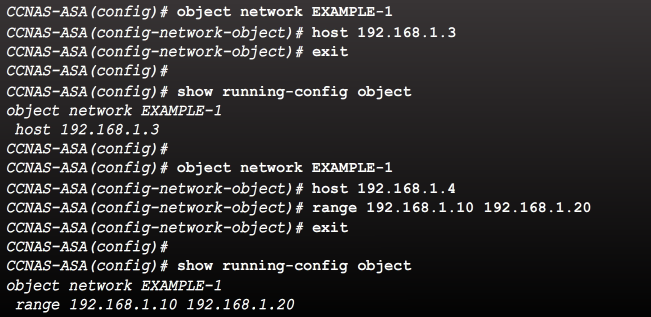
Configuration NTP

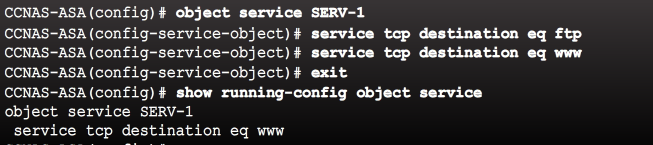


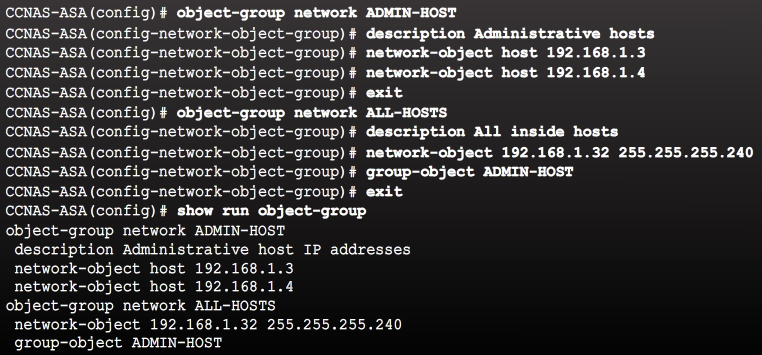
Configuration DHCP

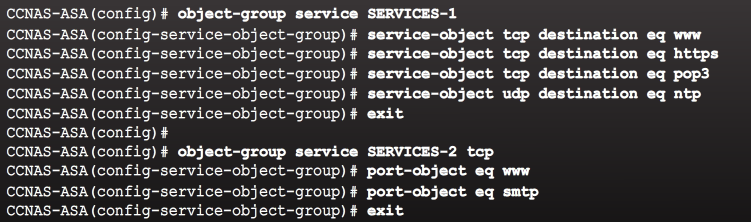


Configuration d’objet

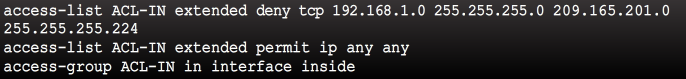


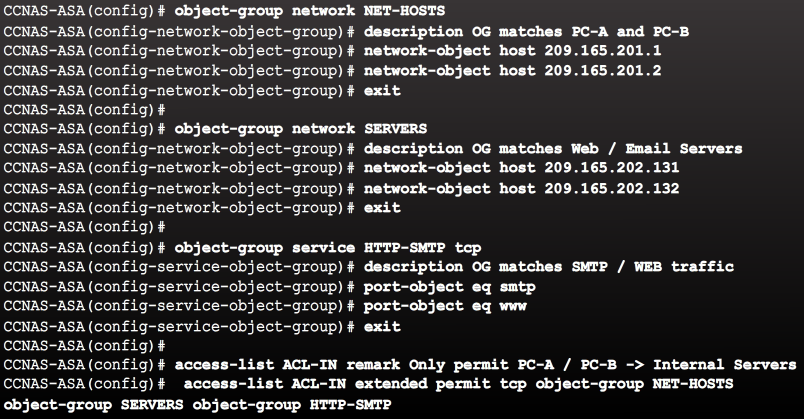




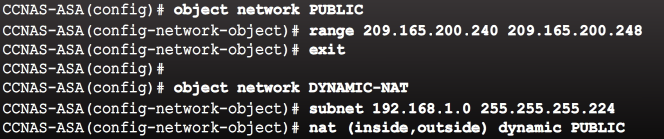


Access list

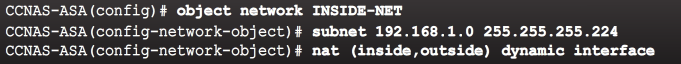


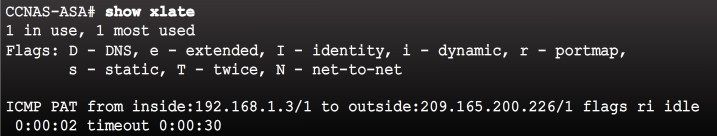


NAT dynamique



PAT

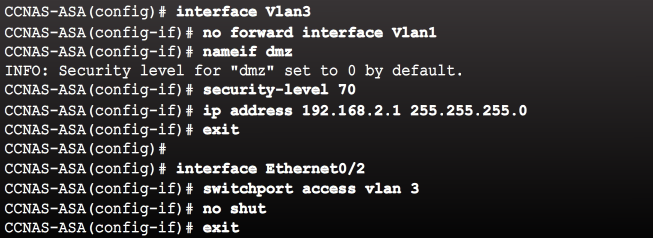




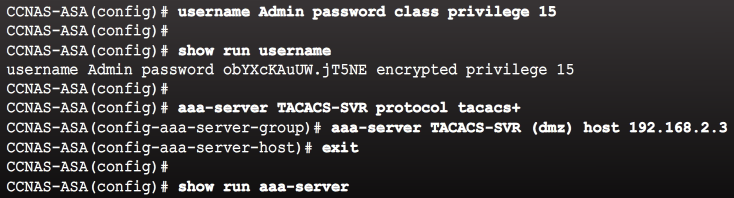
NAT statique

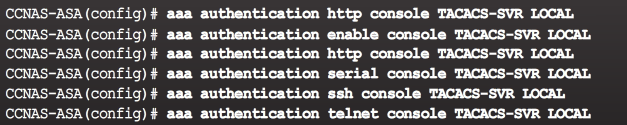


Configuration DMZ avec zone restrict

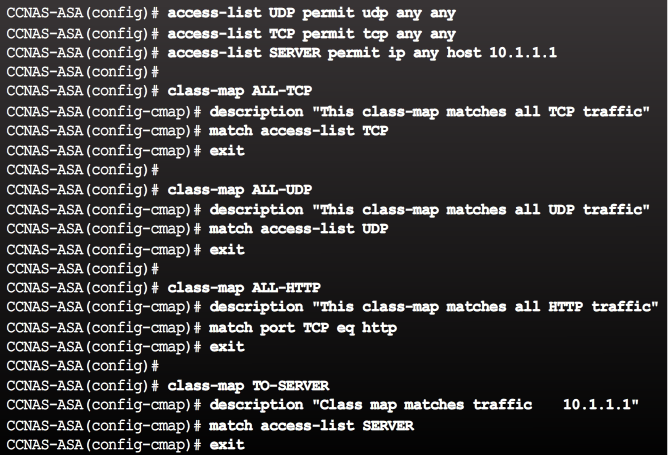


AAA

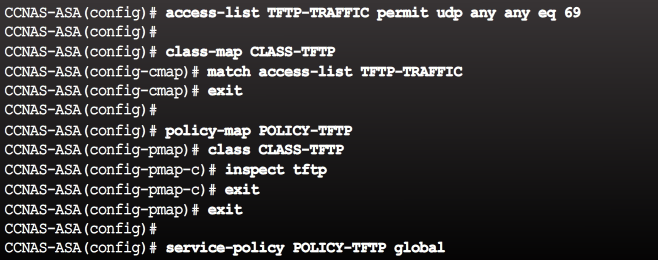




Class Map



Policy



Default inspection

