|  |  |  |  |
| --- | --- | --- | --- |
| Numéro de port | Protocol | Application | Acronyme |
| 20 | TCP | Protocole FTP (File Transfert Protocol) (données) | FTP |
| 21 | TCP | Protocole FTP (File Transfert Protocol) (contrôle) | FTP |
| 22 | TCP | Secure Shell | SSH |
| 23 | TCP | Telnet |  |
| 25 | TCP | Protocole SMTP (Smiple Mail Transfer Protocol) | SMTP |
| 53 | UDP, TCP | Domain Name Service | DNS |
| 67 | UDP | Protocol Dynamic Host Configuration Protocol (serveur) | DHCP |
| 68 | UDP | Protocol Dynamic Host Configuration Protocol (client) | DHCP |
| 69 | UDP | Trivial File Transfer Protocol | TFTP |
| 80 | TCP | HyperText Transfer Protocol | HTTP |
| 110 | TCP | Post Office Protocol | POP3 |
| 143 | TCP | Internet Message Access Protocol | IMAP |
| 161 | TCP | Simple Network Management Protocol | SNMP |
| 443 | TCP | HyperText Transfer Protocol Secure | HTTPS |
| 514 | UDP | Syslog |  |

Quand on réalise un câblage :

Penser à faire un schéma pour savoir quelles IP sont associés à quel port et quel port est relié à un autre.

Objectif d’un router : sélectionner le meilleur chemin

Si pas de destination : route par défaut

Sur un router : RAM, ROM, FLASH, CPU, NVRAM

IOS : Internetwork Operating System

CLI : Command Line Interface

AUI (Attachement Unit Interface) connecteur Ethernet 10mb

Câble console Cisco : UTP inversé : rollover

Afficher les ports et leurs états

sh ip int br

Etat du routage :

show ip route

Associer une IP à un port :

conf t

int nom\_port

ip address adresse\_ip masque

Associer une IP à un VLAN :

conf t

int vlan 1

{(ip address adresse\_IP masque)|(ip address dhcp)}

no shut

Mettre une gateway :

conf t

ip default-gateway adresse\_ip

Créer une IP route :

conf t

ip route adresse\_réseau masque adresse\_prochainRTR [distance Administrative]

(réseau = non connecté sur ce rtr)

Liaison série :

* Synchrone : plus rapide
* Asynchrone : plus lent

Quand on branche un RTR à un CSU/DSU on utilise un câble DTE (série)

Quand on branche un RTR à un autre RTR on utilise un câble DCE (série)

DTE câble male, DCE câble femelle

Pour mettre une horloge sur le port d’une interface série (uniquement pour le câble femelle)

clock rate horloge

Dans la NVRAM : startup-configuration

RAM : running-configuration

Il est possible qu’il n’y ait pas de startup-config, dans ce cas le RTR démarre un system d’initialisation

Afficher la startup-config :

sh start

Afficher la running-config :

sh run

Pour sauvegarder la running-config dans la startup-config :

- copy running-config startup-config

- copy run start

- write

- wr

Mettre un MDP sur le mode enable :

conf t

enable [algorithm-type md5] secret mdp

enable algorithm-type sha256 secret mdp

enable algorithm-type scrypt secret mdp

(Le MDP est crypté en MD5)

Mettre un MDP sur le port console :

conf t

line console 0

login

password mdp

Mettre un MDP sur les connexions Telnet : (vty (virtual teletype) 0 a 4 donc 5 connexions max)

conf t

line vty 0 4

login

password mdp

Discriminez les accès à partir des adresses IP sources :

conf t

access-list 1 permit host adresse\_ip $ crée une access list et ajoute l’IP

line vty 0 4

access-class 1 in $ ajoute l’access list à la connexion VTY

Password encryption : (car les MDP autre que celui du mode enable ne sont pas crypté)

conf t

service password encryption

(crypte en code 7)

Changer le mom d’hôte :

conf t

hostname nom\_hôte

Définir une table d’hôte :

conf t

ip host nom\_hôte adresse\_hôte

Afficher la version de l’IOS

show version

Effacer la startup-config :

erase startup-config

Mettre un motd (Message Of The Day)

banner motd “No unauthorized access allowed violators will be prosecuted to the full extent of the law!”

Empeicher le routeur / switch d’effectuer des recherches DNS

no ip domain-lookup

Activer le protocole RIP et le configurer : (protocole de routage) (les adresse à donner sont les adresse réseau du routeur que l’on veut partager)

conf t

router rip

network adresse\_réseau

Afficher les protocoles utilisés et leurs paramètres

sh ip protocols

Changer la version de RIP (de base la version utilisée est RIPv1)

conf t

router rip

version 1 ou version 2

Auto agrégation de route :

conf t

router rip

auto-summary

Désactiver les annonces RIP sur une interface : (pour éviter par exemple les requêtes inutiles sur un réseau ne comportant par d’autres routeur)

conf t

router rip

passive-interface nom-interface

OSPF vas essayer de voire le topologie de tous les routeurs dans l'architecture

LSP Link state packet (paquet OSPF)

affiche info sur interface

sh int nom\_interface

OSPF: (process-ID : n'importe entre : 1-65535, zone-ID entre 0 et 4 294 967 295)

conf t

router ospf process-ID

network address wildcard-mask area zone-ID

Mettre une interface dans une zone OSPF (méthode équivalente à l’utilisation de "network …" en router ospf X)

conf t

int X

ip ospf process-ID area zone-ID

Definir le routeur-ID OSPF

conf t

router ospf X  
router-id Y

Définir loopback OSPF

conf t

Router ospf X

Interface loopback Y

Annoncer la route par défaut OSPF (sur le routeur connecté à cette route)

conf t

router ospf process-ID

default-information originate

Définir manuellement le cout d’une interface (Y entre 1 et 65535)

conf t

int x

ip ospf cost Y

Changer la bande passante de référence pour le calcul de cout OSPF (X en mbps)

conf t

router ospf process-ID

auto-cost reference-bandwidth X

Définir le nombre maximum de route OSPF au même cout

conf t

router ospf process-ID

maximum-paths X

Définir la priorité OSPF pour l’élection du DR/BDR (higher is better)

conf t

int X

ip ospf priority Y

Définir une interface OSPF comme point-to-point (utile sur les réseaux avec seulement 2 RTR)

conf t

int x

ip ospf network point-to-point

Restart OSPF process

clear ip ospf process

Arrêter le process OSPF (ne supprime pas la configuration mais supprime toutes les relations, table et LSDB)

conf t

router ospf process-ID

shutdown

Changer les hello et death intervall OSPF

conf t

int X

ip ospf hello-interval X(secondes)

ip ospf death-interval Y

Passive interface OSPF :

conf t

router ospf X

passive-interface X

passive-interface default (définit toutes les interfaces en passive par défaut)

no passive-interface X (définit les interfaces non passives)

Afficher les voisins OSPF

sh ip ospf neihbor

Affiche le contenu de la base de données topologique pour tous les routeurs

sh ip ospf database

Affiche le contenu de la base de données topologique pour tous les routeurs du routeur voisin

sh ip ospf database router IP-neighbor

Afficher les interfaces OSPF

sh ip ospf int brief

Supprimer le routing

no ip routing

Activer ou désactiver le routing sur un switch

sdm prefer lanbase-routing

reload

ip routing

DHCP :

Autoriser le passage de requête DHCP : (quand on a un serveur DHCP)

conf t

int InterfaceRéseauAAdresser

ip helper-address adresse\_serveurDHCP

Cree un pool sur RTR

conf t

ip dhcp pool nom\_pool

network ip\_adresse masque

default-router ip\_routeur

dns-server ip\_dns

Exclure des IP du DHCP

conf t

ip dhcp excluded-address adresse\_ip

Voir les baux DHCP

sh ip dhcp binding

Voir les address IP apprise via DHCP sur un switch

sh dhcp lease

NAT Dynamic avec PAT

ip nat inside source list id\_list interface nom\_interface overload

access-list id\_list permit adresse\_reseau masque\_inversé

Indiquer les interfaces

conf t

int nom\_interface\_inside

ip nat inside

int nom\_interface\_outside

ip nat outside

Mapping static de NAT (static)

conf t

ip nat inside source static *inside-local inside-global*

Pool NAT (dynamic)

conf t

ip nat pool *name first-address last-address* netmask *subnet-netmask* (IP global)

ip nat inside source liste cl*-number* pool *pool-name*

Clear dynamic entry from the NAT table :

clear ip nat translation

Show NAT

show ip nat translations

show ip nat statistics

ACL : standar (id access list entre 1 et 99 et 1300 et 1999)

conf t

access-list access\_list\_id [deny|permit} source\_IP [source\_wildcard\_mask] [log]

Affecter access list sur port

conf t

int nom\_port

ip access-group access\_list\_id {in|out}

ACL : entendu (id access llist entre 100 et 199 et 2000 et 2699, protocol : ip icmp tcp udp etc, opérateur : eq(=), neq(), lt(<), gt(>), range(x to y))

conf t

access-list id\_access\_list {permit|deny} protocol adresse\_source wildcard\_masque [opérateur [port]] adresse\_dest wildcard\_masque [opérateur [port]] [log|log-input]

Named ACL

conf t

ip access-list {standar|extended} NAME

permit …

deny …

remark …

Supprimer un ligne spécifique d’une ACL ou ajouter une ligne entre 2

show ip access-list NOM

Regarder le nombre devant la règle

ip access-list {standar|extended} NOM

no NOMBRE

NOMBRE {deny|permit} …

Activer le routage IPv6 : (si non activer mais interface configurée, le RTR fonctionnera comme un host)

conf t

ipv6 unicast-routing

Associer une IPv6 manuellement à un port :

conf t

int nom\_interface

ipv6 address adresse\_ipv6/masque

Associer une IPv6 avec la méthode EUI-64 à un port :

conf t

int X

ipv6 address prefix\_ipv6/masque eui-64

Méthode EUI-64

Subnet Prefix + 1st Half of MAC + FFFE + 2nd half of MAC

(1st Half invert 7th bit (reading left to the right))

Pour inverser le 7e bit, il faut remplacer le 2e chiffre hexadécimal de l’adresse MAC avec celui en correspondance de couleur sur le tableau à gauche

Exemple :  
AA13:ABAB:1001 🡪 A813:ABAB:1001

Donc : Prefix : 2001:DB8:1:1::/64 & Mac : AA13:ABAB:1001 🡪  
2001:DB8:1:1:A813:ABFF:FEAB:1001

|  |  |
| --- | --- |
| 0 | 1 |
| 2 | 3 |
| 4 | 5 |
| 6 | 7 |
| 8 | 9 |
| A | B |
| C | D |
| E | F |

Associer une IPv6 link-local à un port : (adresse link-local : FE80 ::/10 (FE80->FEBF))

conf t

int nom\_interface

ipv6 address adresse\_ipv6 link-local

Associer une IPv6 avec DHCP

conf t

int X

ipv6 address dhcp

Associer une IPv6 avec SLAAC

conf t

int X

ipv6 address autoconfig

Associer une IPv6 automatiquement pour un inter routeur (WAN link)

conf t

int X

ipv6 enable

ipv6 address autoconfig

Associer une IPv6 anycast

conf t

int X

ipv6 address adress\_ipv6/128 anycast

Equivalent "show interface" en IPv6

show ipv6

::1/128 = adresse de bouclage (comme 127.0.0.1)

FC00::/7 + FDFF::/7 = adresse local unique (réseau privé)

FD00 ::/8 = Unique local

FE80::/10 = link-local (FE80->FEBF) (FF02::/16 = link-local multicast address)

FF00::/8 = multicast

2000::/3 = Global unicast (2000->3FFF)

|  |  |  |  |
| --- | --- | --- | --- |
| Short Name | Multicast Address | Meaning | IPv4 Equivalent |
| All-nodes | FF02::1 | All-nodes (all interfaces that use IPv6 that are on the link) | 224.0.0.1 |
| All-routers | FF02::2 | All-routers (all IPv6 router interfaces on the link) | 224.0.0.2 |
| All-OSPF, All-OSPF-DR | FF02::5, FF02::6 | All OSPF routers and all OSPF-Designated routers | 224.0.0.5, 224.0.0.6 |
| RIPng Routers | FF02::9 | All RIPng routers | 224.0.0.9 |
| EIGRPv6 Routers | FF02::A | All routers using EIGRP for IPv6 | 224.0.0.10 |
| DHCP Relay Agent  (solicited-node multicast addresses) | FF02::1:2 | All routers acting as a DHCPv6 relay agent | None |

IPv4 Network/Subnet/Host ⬄ IPv6 Global routing prefix / Subnet / InterfaceID

IPv6 NDP (Neighbord Discovery Protocol) replace IPv4 ARP   
NDP fonctionne avec des adresse multicast FF02::1:FFXX:XXXX ou X sont les 6 derniers digit de l’adresse recherché

IP route IPv6

conf t

ipv6 route IPv6\_network/masque netx\_hop

IP route IPv6 link-local (X = interface)

conf t

ipv6 route IPv6\_network/masque X netx\_hop\_link\_local

IP route IPv6 serial link (X = interface)

conf t

ipv6 route IPv6\_network/masque X

Sécuriser le routeur :

auto secure

Changer la taille minimale de mot de passe : (X = nombre de caractères)

security password min-length X

Bloquer les tentatives de connexion pendant X seconds après Y échecs de connexion en l’espace de Z seconds :

login block-for X attempts Y within Z

Mettre un timeout qui ferme la connexion au bout de Y minutes d’inactivité (X = vty ou console)

line X

exec-timeout Y

Activer SSH : (X= nom du domaine IP du réseau, Y= nbr de bits entre 360 et 2048) (la connexion ne fonctionneras qu’avec SSH)

conf t

ip domaine-name X

crypto key generate rsa general-keys modulus Y

line vty 0 4

transport input ssh

Cree des utilisateurs et les utiliser pour la connexion (A = nom d’utilisateur et C son MDP, B est le niveau de privilège (15 si on le ne spécifie pas, 0 le plus bas et 15 le plus fort))

conf t

username A privilege B [algorithm-type md5] secret C

username A privilege B algorithm-type sha256 secret C

username A privilege B algorithm-type scrypt secret C

Activer l’utilisation des utilisateurs : (X = vty ou console)

line X

login local

Activer telnet et SSH :

conf t

line vty 0 4

transport input telnet ssh

Paramétrer plusieurs interfaces à la fois :

conf t

interface range f0/14 , f0/7-24 , g0/1-2

CDP : permet de découvrir les éléments Cisco environnant :

show cdp neighbors [type number]

show cdp neighbors detail

show cdp entry *name*

Désactiver CDP partout

conf t

no cdp run

Désactiver CDP sur une interface

conf t

int X

no cdp enable

Changer les temps de CDP

conf t

cdp timer *secondes* (change l’intervalle entre chaque requêtes CDP default 60)

cdp holdtime *secondes* (change le temps que l’équipement garde l’info default 180)

LLDP : permet de découvrir les éléments environnant : (comme cdp mais IEEE 802.1AB)

show lldp neighbors

show lldp neighbors detail

show lldp entry *hostname*

Désactiver LLDP partout

conf t

no lldp run

Désactiver LLDP sur une interface

no lldp transmit (transfert de messages)

no lldp receive (process de messages)

Changer les temps de LLDP

conf t

lldp timer *secondes* (change l’intervalle entre chaque requêtes LLDP default 30)

lldp holdtime *secondes* (change le temps que l’équipement garde l’info default 120)

Autoriser l’envoi de messages de log à la session distante (SYSLOG) (SSH, TELNET) :

terminal monitor

Afficher les logs

show logging

Disable timestamp in log and enable sequence numbers in logs

conf t

no service timestamps

service sequence-numbers

Définir un serveur Syslog

conf t

logging host {address|hostname}

Enable logging

logging {console|monitor|buffered}

Chose logging level (trap is for Syslog)

logging {console|monitor|buffered|trap} {level-name|level-number}

Activer ou desactiver le mode debug

debug ip icmp

no debug ip icmp

undebug ip icmp

undebug all

NTP

clock set 22:33:30 12 May 2020

conf t

clock timezone UTC +1

clock summer-time EDT recurring

NTP server only (stratum-level = accuracy of the clock, lower is beter(1-15), 8 default, increase 1 each bound)

conf t

ntp master [stratum-level]

ntp source loopback X (non obligatoire mais permet l’utilisation de loopback au lieux d’interfaces)

Définir un serveur NTP (multiplier la commande pour ajouter plusieurs sources)

conf t

ntp server {address|hostname}

Mettre plusieur adresse IP sur un port en function du vlan (A et B des vlan) (sous interface non-obligatoire pour le VLAN1 si utilisé comme NATIVE vlan) (ROAS : Router On A Stick)

int g0/0  
no shut  
int g0/0.1

encapsulation dot1q A  
ip address X Y

int g0/0.2

encapsulation dot1q B

ip address V W

Transformer l’interface d’un switch en routed interface

conf t

int X

no switchport

MPLS :

conf t

int X

mpls ip

sh mpls forwarding-table

Agrégation de liens sur un switch

conf t

int X

channel-group Y mode {auto[non-silent]|desirable[non-silent]|on}

Désactiver spanning-tree sur un port

conf t

spanning-tree portfast bpduguard default

int X

spanning-tree portfast

Activer RSTP (Rapid Spanning-Tree)

conf t

spanning-tree mode rapid-pvst

Port security bloquer l’accès (optionnel)

conf t

int X

switchport mode {access|trunk}

switchport port-security

switchport port-security maximum Y (nbr of MAC-ADDRESS)

switchport port-security violation {protect|restrict|shutdown}

switchport port-security limit rate invalid-source-mac (set rate limit for bad packet)

switchport port-security mac-address Z

switchport port-security mac-address sticky (learn the mac address dynamically)

Afficher le port security

sh port-security interface

sh port-security address interface X

sh port security address

Reactiver un port err-disabled (X = secondes)

errdisabled recovery cause psecure-violation (reactive tout les port en err-disable)

errdisabled recovery interval X (time to wait before recovering the interface)

Activer BGP (BGP = Border Gateway Protocol, AS = Autonomous System)

router bgp X (X = numero de l’AS)

neighbor IP remote-as Y (Y = numéro d’AS distant, IP = IP routeur distant)

Afficher les infos BGP

sh ip bgp summary

Déclarer un réseau au BGP

router bgp X

network IP mask MASQUE

Déclarer le BGP aux autre routeur du réseau

router ospf X

redistribute bgp Y subnets (Y = numéro de l’AS)

Déclarer les supernet BGP (nécessite la déclaration d’un network)

router bgp X

aggregate-address IP\_SUPERNET MASK\_SUPERNET summary-only

Autre moyen de declarer un supernet au BGP

ip route IP\_SUPERNET MASK\_SUPERNET null 0

router bgp X

network IP\_SUPERNET mask MASK\_SUPERNET

Configurer un iBGP (internet BGP, pour un réseau de transit par exemple)

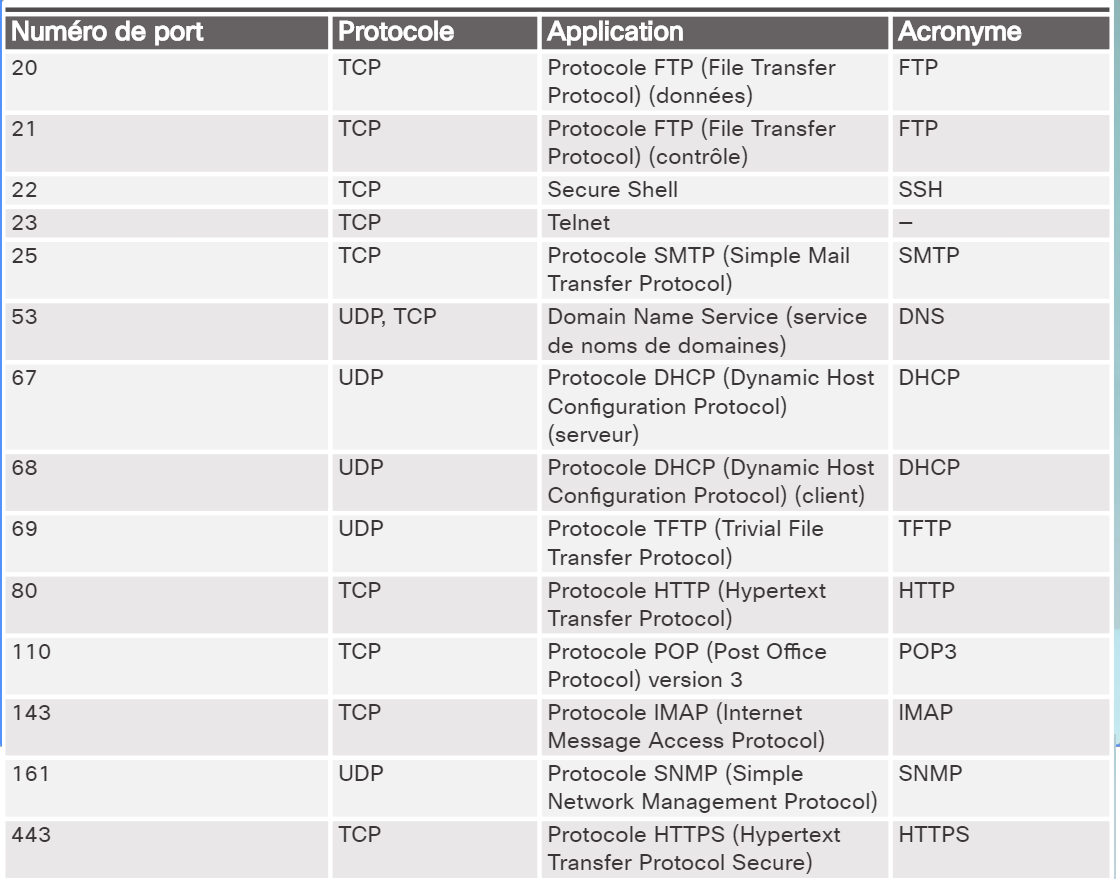
router bgp X (X = numéro de l’AS du réseau de transit)

neighbor IP\_RTR\_DISTANT remote-as X

neighbor IP\_RTR\_DISTANT next-hop-self

Afficher les infos en WiFi

sh controlers dot11Radio X



Configurer plusieurs ssid avec un vlan special

dot11 ssid NOM\_SSID

vlan X

authentication open (réseau ouvert)

mbssid guest-mode (réseau annoncé par l’AP)

Annoncer 2 ssid

int dot11radioX

mbssid

ssid X

ssid Y

int dot11radioX.1

encapsulation dot1q ID\_VLAN1

bridge-group ID\_VLAN1

int dot11radioX.2

encapsulation dot1q ID\_VLAN2

bridge-groupe ID\_VLAN2

int FX.1

encapsulation dot1q ID\_VLAN1

bridge-group ID\_VLAN1

int FX.2

encapsulation dot1q ID\_VLAN2

bridge-groupe ID\_VLAN2

WiFi (http interface)

Radius server :

Security > AAA > Radius > Authentication

Dynamic Interface : (used to connect WLC to a VLAN on the wired network, when you create a vlan, you will bind the dynamic interface and vlan to a wireless network)

Controller > Interface

Puis éditer l’interface pour configurer les adresses IP

WLAN :

WLANs > Create New

Puis éditer le WLAN pour configurer le fonctionnement et sélectionner la Dynamic Interface

WLAN Security :

WLANs > Edit > Security

Pour l’utilisation de radius, de base il feras les requetes par le port de management, pour utiliser le port virtuel, cocher la case « Radius Server Overwrite interface »

QoS :

WLANs > Edit > QoS

Platinium (voice)

Gold (Video)

Silver (Best effort)

Bronze (background)

Exclude a client :

Security > Wireless Protection Policies > Client Exclusion Policies

Enable management from WiFi client

Management > Mgmt Via Wireless

Mettre un port en mode trunk en selectionnant le protocol ISL (Cisco) dot1q (802.1q)

conf t

int X

switchport trunk encapsulation dot1q

switchport mode trunk

Ajouter un serveur Radius sur un Switch

conf t

aaa new-model

aaa authentication login default line group radius

line X

login authentication default

radius-server host IP auth-port PORT acct-port PORT [key CLEF]

aaa group server radius NOM\_SERVER

server IP

aaa accounting network default start-stop group radius

aaa authorization network default group radius

aaa authorization exec default group radius

aaa authorization exec default group radius if-authenticated

radius-server vsa send

Serveur VTP sur un catalyst 5505

set vtp domain NOM\_DOMAIN

set vlan ID name NOM

Client VTP

conf t

vtp mode client

vtp domain NOM\_DOMAIN

Sur un catalyst 5505 set ip et vlan sur sc0 et VLAN, TRUNK

set interface sc0 IP MASK

set interface sc0 VLAN\_ID

set trunk PORT on isl VLAN

set vlan ID\_VLAN INTERFACE

Sur un catalyst 5505, activer VMPS (serveur)

set vmps tftpserver 10.2.0.170 vmps-config-database.txt

set vmps state enable

Client VMPS

conf t

vmps server IP

Activer l’agent SNMP

conf t

snmp-server community public

Définir des informations

conf t

snmp-server NOM\_VARIABLE VALEUR

Créer une communauté SNMP

conf t

snmp-server community NOM [RO|RW]

Activer les trap SNMP

conf t

snmp-server enable traps snmp NOM\_TRAP

Nomer un vlan dans un firewall

conf t

int vlan X

nameif NOM

DHCP dans un firewall

dhcpd address 192.168.1.2-192.168.1.254 inside

dhcpd enable inside

dhcpd dns IP\_DNS

Route par défaut dans un firewall

conf t

route outside 0.0.0.0 0.0.0.0 IP

Autoriser les ping dans un firewall

conf t

access-list 101 permit icmp any any echo-reply

access-group 101 in interface outside

Translation d’adresse dans un firewall

conf t

static (DMZ,outside) 118.218.0.100 192.168.2.100 netmask 255.255.255.255

Autoriser les flux HTTP vesr un serveur web interne

conf t

access-list 101 permit tcp any host 118.218.0.100 eq www

Définir le temsp q’un switch retien une adresse mac

conf t

mac address-table aging-time TEMPS [vlan ID\_VLAN]

Vider la table d’adresse mac

clear mac-address-table dynamic vlan ID\_VLAN

clear mac-address-table dynamic interface ID\_INT

clear mac-address-table dynamic address MAC\_ADDRESS

Desactiver VTP

conf t

vtp mode {transparent|off}

Définir un vlan pour la voix VoIP (cdp doit être activé)

conf t

vlan 10

vlan 11

int range F0/1-4

switchport mode access

switchport access vlan 10

swicthport voice vlan 11

Définir les mods spanning tree

conf t

spanning-tree mode {mst|pvst|rapid-pvst}

Définir le switch root primaire et secondaire spanning tree

spanning-tree vlan X root {primary|secondary}

Afficher les infos IP sur un host :

Windows :

ipconfig

ipconfig /all

netstat -rn (table de routage)

macOS :

ifconfig

networksetup -getinfo

networksetup -getdnsserver

netstat -rn (table de routage)

Linux :

ifconfig

ip address

netstat -rn

ip route

DHCP Snooping

conf t

ip dhcp snooping

ip dhcp snooping vlan X

no ip dhcp snooping information option (when the switch is NOT a DHCP Relay agent)

int X

ip dhcp snooping trust

Limiter le nombre de requêtes DHCP par sec

conf t

int X

ip dhcp snooping limit rate Y

Automatic recovery err-disable of snooping limit rate (X en sec)

conf t

errdisable recovery cause dhcp-rate-limit

errdisable recovery interval X

Afficher les info DHCP Snooping

show ip dhcp snooping

Dynamic ARP Inspection (DAI) (need DHCP Snooping and/or ARP ACL)

conf t

ip arp inspection vlan X

int Y

ip arp inspection trust

Limoter le nombre de requetes ARP (X = nombre de req, Y = intervalle en sec)

conf t

int X

ip arp inspection limit rate X [burst interval Y]

Automatic recovery err-disable of arp inspection limit rate (X en sec)

conf t

errdisable recovery cause arp-inspection

errdisable recovery interval X

Ajouter des étapes de validation DAI (optionnel)

conf t

ip arp inspection validate {[dst-mac] [src-mac] [ip]}

Afficher les info DAI

show ip arp inspection

Distancees administratives des différents types de route

|  |  |
| --- | --- |
| Route Type | Administration distance |
| Connected | 0 |
| Static | 1 |
| BGP (external routes [eBGP]) | 20 |
| EIGRP (internal routes) | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EIGRP (external routes) | 170 |
| BGP (internal routes [iBGP]) | 200 |
| DHCP default route | 254 |
| Unusable | 255 |

Afficher les disques :

show file systems

Vérifier l’intégrité d’un IOS avec MD5

verify /md5 *file-name* *clef-MD5*

Définir les identifiants FTP

conf t

ip ftp username *username*

ip ftp password *password*

Selectionner l’IOS

boot system flash [flash-fs:] [filename]

boot system {tftp|ftp} filename [ip-address]