SOMMAIRE

Mode ROMMON

Le mode ROMMON est un IOS simplifié situé dans la ROM. Il est accessible lorsque le routeur ne peut pas démarrer, ou si une des combinaisons de touches suivantes interrompt la séquence de boot normale :

- CTRL + PAUSE
- CTRL + SHIFT + PAUSE (PAUSE = BREAK)
- CTRL + FN + PAUSE

En fonction des capacités de l'EAR, il existe 2 façons d'installer un IOS :

- TFTP
- XMODEM

Vérifiez si la commande tftpdnld est présente

rommon > ?

Transfert TFTP

rommon > dir flash: liste la mémoire flash
rommon > meminfo infos relatives à la mémoire principale

Configurez les variables d'environnement pour le transfert TFTP

rommon > set affiche les variables
rommon > NOM_VARIABLE=VALEUR configure une variable
rommon > unset NOM_VARIABLE efface une variable

Les variables à configurer sont :

IP_ADDRESS : @IP de la première interface du routeur
IP_SUBNET_MASK : @MASK
DEFAULT_GATEWAY : @GW configure une gw si besoin
TFTP_SERVER : @IP_SVR-TFTP
TFTP_FILE : nom de l'IOS à télécharger

rommon > tftpdnld lance le transfert TFTP

Acceptez l'effacement total de la flash

Transfert XMODEM

rommon > confreg configuration du registre

do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:

disable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: y mettre 115200

change the boot characteristics? y/n [n]:

rommon > reset

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

rommon > xmodem NOM_IOS.bin

Répondez « oui » aux questions

Ready to receive file …

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 !!

Mode privilégié

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

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

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

Manipuler les fichiers

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

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

Remettre en configuration usine

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

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

Sauvegarder / Restaurer la configuration / l'IOS

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

Router(config)#boot system flash:NOM_IOS.bin             IOS à charger au démarrage

Router(config)#archive
Router(config-archive)#path flash:                       emplacement de sauvegarde local
Router(config-archive)#path tftp://SVR-TFTP//$h.cfg      sauvegarde sur serveur TFTP
Router(config-archive)#path scp://USER :MDP@SVR-SCP//$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
Router(config-archive)#maximum nbre_backup               nbre de sauvegardes conservées
Router(config-archive)#write-memory                      crée sauvegarde si enregistrement
Router(config-archive)#time-period 1440 (en min)         crée sauvegarde toutes les 24H

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

Router#show archive config                               affiche les sauvegardes effectuées
Router#show archive config differences | incremental-diffs …
```

Redémarrer

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

Paramétrer la date et l'heure

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

Réinitialisation de paramétres

Router#clear arp-cache — vide le cache des @MAC
Router#clear ip ospf process_id — relance le processus OSPF
Router#clear bgp all num_AS — relance le BGP
Router#clear ip bgp * — relance le BGP
Router#clear ip route * — vide la table de routage
Router#clear access-list counters — remise à zéro des compteurs d'utilisation
Router#clear ip accounting

Visualisation des configurations et états

Router#show running-config — affiche la config courante en RAM
Router#show running-config partition line|snmp|router|access-list
affiche une partie de la config courante en RAM
Router#show startup-config — affiche la config persistante en NVRAM
Router#show config history — affiche l'historique d'enregistrement des confs
Router#show config id detail — affiche les infos du dernier enregistrement de la conf
Router#show version — affiche la version de l'IOS

Router#show adjacency — affiche toutes les @IP des équipements adjacents
Router#show arp — affiche la table de relation @MAC et @IP

Router#show telephony-service — affiche l'état du serveur de VOIP
Router#show voice register all
Router#show voice register global

Test de la connectivité

Router#ping @IP — message ICMP standard
Router#ping
taper ping puis entrée puis renseigner les paramètres étendus
ou
Router#ping @IP_dest source @IP_source repeat nbre_paquets size taille_paquet_bits df-bit
df-bit permet de spécifier dans l'entête du paquet qu'il ne doit pas être fragmenté

ou

Router#traceroute @IP/@FTP/@HTTP — détermine l'itinéraire emprunté
Router#traceroute — taper traceroute et renseigner les paramètres étendus

Mode de configuration globale

```
Router#configure terminal
Router(config)#
```

Nommer le routeur

```
Router(config)#hostname nom_routeur
```

Afficher une bannière

```
Router(config)#banner motd ^

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

        NOM DU ROUTEUR
^
Router(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 '@'

Configurer des alias de commandes

Router(config)#alias configure show do show
Router(config)#alias configure sh do sh
Router(config)#alias configure ping do ping
Router(config)#alias configure trace do trace
Router(config)#alias configure wri do wri

Activer le chiffrement de type 7 (propriétaire CISCO)

Router(config)#service password-encryption chiffre les mdp des accès console, vty …

Router(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

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

Verrouillage session

Router(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 compte

Router(config)#username nom_user privilege niveau password num mdp mdp en clair
Router(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

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

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

Router(config)#username releve privilege niveau one-time secret releve
crée un compte à usage unique

Authentication Authorization Accounting

Activation AAA

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

Gestion des droits d'accès par VIEW

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

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

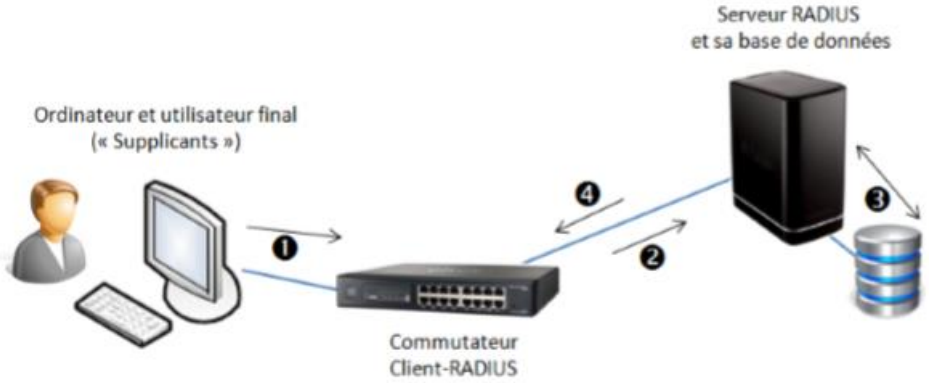
Router(config-view)#exit

Affecter la VIEW

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

AAA avec RADIUS

Authentification Autorisation Accounting
Remote Authentication Dial-In User Service



Activation AAA

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

Configuration des serveurs RADIUS

Router(config)#ip radius source-interface fastethernet|gigabitethernet|vlan slot/port|num
Router(config)#radius-server host @IP_SVR-RADIUS timeout sec retransmit sec 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

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

Router(config)#aaa authentication login default|nom_liste_authentif_CONSOLE line
Utilise le mdp de l'interface de connexion (console, vty …)
Router(config)#aaa authentication login default|nom_liste_authentification group radius local
Utilise les serveurs RADIUS puis les comptes locaux si SVR injoignable
Router(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
Router(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

Router(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
Router(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
Router(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

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

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

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

Fonctions de test AAA

```
Router#test aaa group radius NOM-USER MDP legacy
```

VLAN

Note: Gestion des VLANs de manière statique

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

Router#show vlan-switch brief          affiche l'état et les ! associés à tous les VLANS
```

SNMP (Simple Network Management Protocol) V2c/V3

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

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

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

Router(config)#snmp-server host @IP_SUPERVISION version 3 auth user
Router(config)#snmp-server host @IP_SUPERVISION informs version 3 auth user
Router(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)

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

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

Router(config)#snmp-server source-interface traps fastethernet|gigabitethernet slot/port
Router(config)#snmp-server source-interface informs fastethernet|gigabitethernet slot/port
```

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

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

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


Router(config)#snmp-server enable traps                     active toutes les notifications
Router(config)#snmp-server enable traps snmp authentication warmstart coldstart
Router(config)#snmp-server enable traps linkdown linkup     lien up et down
Router(config)#snmp-server enable traps config              configuration modifiée
Router(config)#snmp-server enable traps config-copy
Router(config)#snmp-server enable traps config-ctid
Router(config)#snmp-server enable traps syslog              SYSLOG
Router(config)#snmp-server enable traps rtr                 Response Time Reporter pour IPSLA
Router(config)#snmp-server enable traps tty                 accès SSH/TELNET
Router(config)#snmp-server enable traps authenticate-fail   authentifications ratées
Router(config)#snmp-server enable traps envmon              notifications matérielles
Router(config)#snmp-server enable traps memory bufferpeak
Router(config)#snmp-server enable traps event-manager
Router(config)#snmp-server enable traps cpu threshold
Router(config)#snmp-server enable traps flash insertion removal
Router(config)#snmp-server enable traps vlancreate
Router(config)#snmp-server enable traps vlandelete
Router(config)#snmp-server enable traps vlan-membership
Router(config)#snmp-server enable traps mac-notification
Router(config)#snmp-server enable traps port-security
Router(config)#snmp-server enable traps auth-framework sec-violation

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


Router#show snmp                    affiche l'état de SNMP
Router#show snmp ifmib ifindex      affiche les n° d'index SNMP associés aux interfaces
```

Journalisation en LOCAL / vers SYSLOG

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

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

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

Router#show logging                                 affiche l'état de la journalisation
```

Enregistrement des changements de configuration

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

Filtrage des remontées SYSLOG

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

NTP = Network Time Protocol

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

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

à paramétrer sur l'EAR faisant office de serveur NTP :
```
Router(config)#ntp master num_stratum
```
num_stratum = niveau hiérarchique du serveur dans l'architecture des synchronisations

à paramétrer sur l'EAR client du serveur NTP :
```
Router(config)#ntp server @NTP_SERVER source nom_interface slot/port key num_clé version X
```
@IP du serveur de temps de référence

Définir une route statique

@RSO_distant peut englober plusieurs RSO à joindre, c'est un résumé de routes
```
Router(config)#ip route @RSO_distant @MASK_RSO_distant @next_hop name NOM
Router(config)#ip route @RSO_distant @MASK_RSO_distant @next_hop name NOM tag num
Router(config)#ip route @RSO_distant @MASK_RSO_distant @next_hop name NOM metric
Router(config)#ip route 0.0.0.0 0.0.0.0 @next_hop name ROUTE_PAR_DEFAUT
```
route par défaut -> permet de joindre tous les RSO distants

```
Router(config)#ip route @RSO_distant @MASK_RSO_distant type_interface slot/port  name NOM
```
Cas d'une liaison série point à point (HDLC/PPP) : pas de nexthop, utiliser l'interface de sortie

```
Router#show ip route                affiche la table de routage
Router#show ip route static         affiche la table de routage statique
```

Monitoring de port / VLAN

```
Router(config)# monitor session num source interface fastethernet slot/port
        ou
Router(config)# monitor session num source vlan id_vlan
Router(config)# monitor session num destination interface fastethernet slot/port
Router(config)# monitor session num filter vlan id_vlan      filtre par VLAN


Router#show monitor session num      affiche les paramètres de la session de monitoring
```

DHCP

Attribution dynamique

```
Router(config)# ip dhcp pool NOM_PLAGE                  nom de la plage DHCP
Router(dhcp-config)# network @RSO @MASK                 plage d'@IP définie par l'@RSO
Router(dhcp-config)# default-router @IP_GW
l'@IP_GW peut être l'@IP de l'interface distribuant  les @IP, cette @IP servira de passerelle
Router(dhcp-config)# option code_DHCP ip @IP            optionnel
par ex le code 150 est relatif aux terminaux VOIP récuperant leur configuration à l'@IP
spécifiée ; cette @IP peut être l'@IP_GW, ici c'est le routeur qui fournira la configuration
(cf.VOIP)
Router(dhcp-config)# domain-name domaine
Router(dhcp-config)# dns-server @IP-DNS1 @IP-DNS2
Router(dhcp-config)#lease nbre_jours | infinite         durée du bail DHCP
Router(config)# ip dhcp excluded-address @IP            @IP exclue de la distribution

Router(config-if)#ip helper-address @IP-SVR-DHCP
Appliquée à l'interface du côté du client effectuant des requêtes DHCP vers l'adresse de
broadcast limité 255.255.255.255 (ne traversant pas les RTR par défaut), cette commande
permet au RTR recevant ces requêtes de les relayer vers un SVR DHCP distant
```

Attribution statique

```
Router(config)# ip dhcp pool NOM_PLAGE                  nom de la plage DHCP
Router(dhcp-config)# host @IP @MASK
Router(dhcp-config)# client-identifier @MAC
Attention au format de l' => ex : 01XX.XXYY.YYZZ.ZZ pour l'@MAC XXXX.YYYY.ZZZZ
Router(dhcp-config)# default-router @IP_GW
l'@IP_GW peut être l'@IP de l'interface distribuant  les @IP, cette @IP servira de passerelle
Router(dhcp-config)# domain-name domaine
Router(dhcp-config)# dns-server @IP-DNS1 @IP-DNS2


Router#show ip dhcp binding          affiche les attributions du serveur DHCP - @IP/@MAC
```

VOIP

Configuration du service de téléphonie IP ou Call Manager Express

Note : la procédure suivante est à reproduire sur le routeur proposant le service de téléphonie IP de chaque site

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones num                nombre d'IP Phone à gérer
Router(config-telephony)#max-dn num                     nombre de répertoires à gérer
Router(config-telephony)#ip source-address @IP-RTR port num
@IP-RTR = passerelle pour les IP Phone / port = 2000 par défaut
Router(config-telephony)#system message TEXTE

Router(config-telephony)#auto-reg-ephone                [auto enregistrement des ephones]
Router(config-telephony)#auto assign 1 to 9
[affecte automatiquement les lignes 1 à 9 aux ephones qui s'enregistrent]

Router(config-telephony)#shutdown                       éteint le service de VOIP
Router(config-telephony)#exit
```

Configuration des IP Phone SCCP

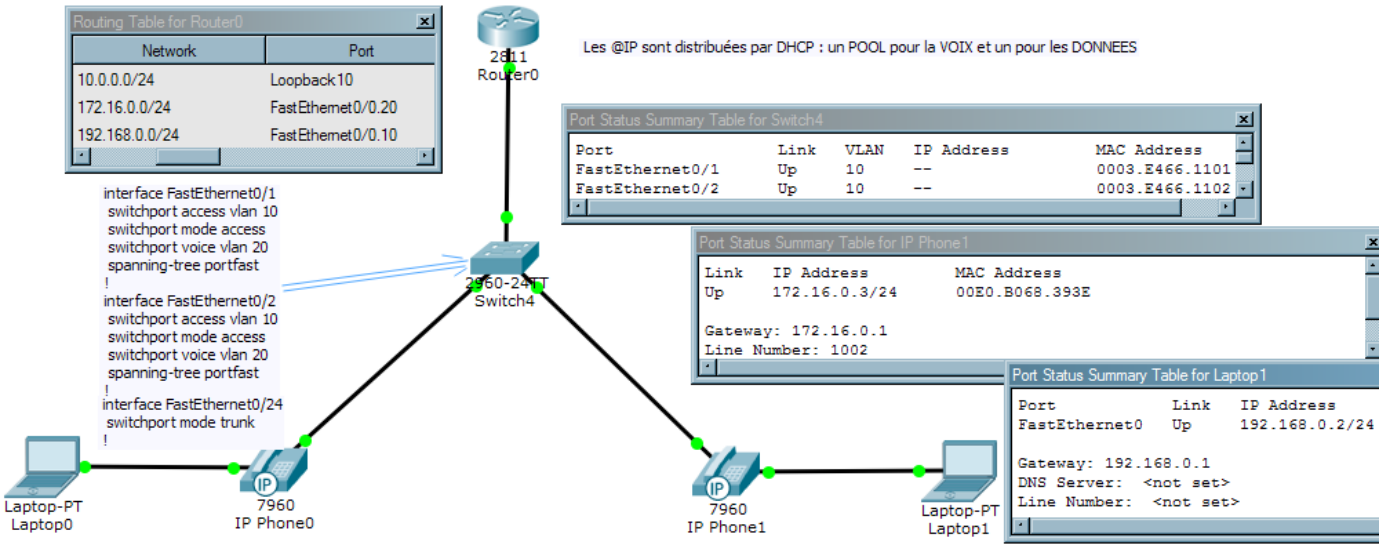
Note : la procédure suivante est à reproduire pour chaque IP Phone géré par le routeur proposant le service de téléphonie IP de chaque site (ephone = ethernet phone)

```
Router(config)#ephone-dn num_dn
Router(config-ephone-dn)#name NOM
Router(config-ephone-dn)#description DESCRIPTION
Router(config-ephone-dn)#label LABEL
Router(config-ephone-dn)#number num_tel
Router(config-ephone-dn)#exit

Router(config)#ephone num
Router(config-ephone)#mac-address XXXX.YYYY.ZZZZ
Router(config-ephone)#type type                         types: CIPC, séries 6xxx, 7xxx, ATA
Router(config-ephone)#button num-touche:num_dn          affecte ligne num_dn>>bouton num
Router(config-ephone)#reset                             redémarre l'ephone
Router(config-ephone)#restart                           redémarre l'ephone complétement
```

Exemple pour deux IP Phone situés dans un même LAN :

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 1001
Router(config-ephone-dn)#exit
```

```
Router(config)#ephone 1
Router(config-ephone)#mac-address 0006.2AA1.B5C3
Router(config-ephone)#type 7960                          autres types : CIPC, ATA …
Router(config-ephone)#button 1:1
Router(config-ephone)#exit

Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 1002
Router(config-ephone-dn)#exit

Router(config)#ephone 2
Router(config-ephone)#mac-address 0001.C913.AD4B
Router(config-ephone)#type 7960
Router(config-ephone)#button 1:2
Router(config-ephone)#exit

Router#show ephone                                affiche les IP Phone enregistrés
Router#show ephone attempted-registrations        affiche les IP Phone en attente d'enregistrement
```



Configuration du service de VOIP en mode Call Manager Express

Note : la procédure suivante est à reproduire sur le routeur proposant le service de téléphonie IP de chaque site

```
Router(config)#voice service voip
Router(config-voicecard)# allow-connections sip to sip
Router(config-voicecard)# sip
Router(config-serv-sip)# registrar server
Router(config-serv-sip)#exit
Router(config-voicecard)#exit

Router(config)#voice register global
Router(config-register-global)# mode cme
Router(config-register-global)# source-address @IP-RTR port num
@IP-RTR = passerelle pour les IP Phone / port = 5060 par défaut
Router(config-register-global)# max-dn num                nombre d'IP Phone à gérer
Router(config-register-global)# max-pool num              nombre de répertoires à gérer
Router(config-register-global)# authenticate realm local  authentification locale
```

Configuration des IP Phone SIP

Note : la procédure suivante est à reproduire pour chaque SIP Phone géré par le routeur proposant le service de téléphonie IP de chaque site

```
Router(config)#voice register dn num_dn
Router(config-register-dn)# number NUM
Router(config-register-dn)# name NOM
Router(config-register-dn)# label LABEL
Router(config-register-dn)#exit

Router(config)#voice register pool num_pool
Router(config-register-pool)# id mac XXXX.YYYY.ZZZZ
Router(config-register-pool)# number 1 dn num_dn                affecte num_dn à la ligne 1
Router(config-register-pool)# username voip10 password voip10   définit le compte SIP utilisé
Router(config-register-pool)# codec NOM-CODEC                   codec utilisé par SIP phone
Router(config-register-pool)#exit
```

Exemple pour deux SIP Phone situés dans un même LAN :

```
Router(config)#voice register dn 1
Router(config-register-dn)# number 1010
Router(config-register-dn)# name POSTE 1010
Router(config-register-dn)# label SOFTPHONE 1010
Router(config-register-dn)# exit
```

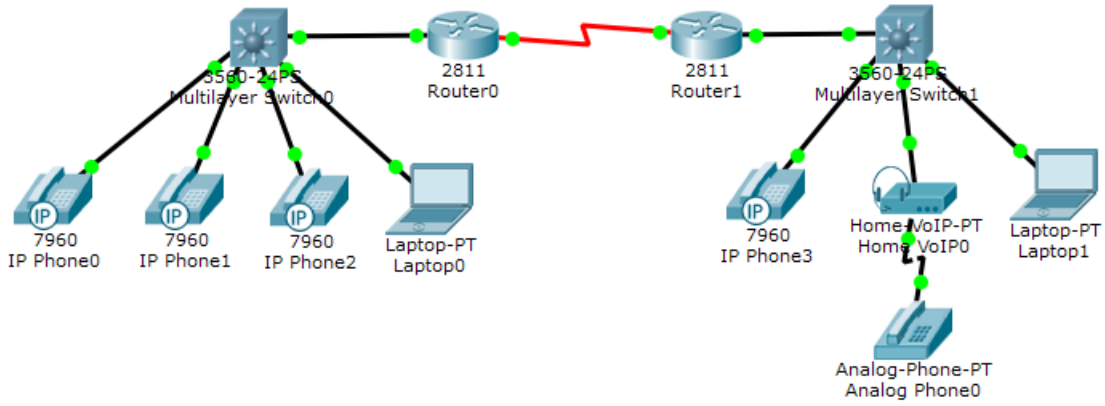
```
Router(config)#voice register pool 1
Router(config-register-pool)# id mac 000c.29b3.02af
Router(config-register-pool)# number 1 dn 1
Router(config-register-pool)# username voip10 password voip10
Router(config-register-pool)# codec g711alaw
Router(config-register-pool)# exit

Router(config)#voice register dn 2
Router(config-register-dn)# number 1020
Router(config-register-dn)# name POSTE 1020
Router(config-register-dn)# label SOFTPHONE 1020
Router(config-register-dn)# exit

Router(config)#voice register pool 2
Router(config-register-pool)# id mac 000c.29cc.a0f0
Router(config-register-pool)# number 1 dn 2
Router(config-register-pool)# username voip20 password voip20
Router(config-register-pool)# codec g711alaw
Router(config-register-pool)# exit
```

Routage intersite VOIP

```
Router(config)#dial-peer voice num voip
Router(config-dial-peer)#destination-pattern [2-4]…  n° à 5 chiffres commençant par 2|3|4
Router(config-dial-peer)#session target ipv4:@IP_NEXTHOP
Router(config-dial-peer)#exit
```

Exemple de dial peer :

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern 20..      n° à 4 chiffres commençant par 20
Router(config-dial-peer)#session target ipv4:30.30.30.2
Router(config-dial-peer)#exit
```



Configuration des lignes analogiques

Il existe 2 types de voice port analogique fournissant courant et tonalité :

- les FXO -- Foreign eXchange Office : c'est l'interface directement reliée à l'opérateur téléphonique, de type Réseau Téléphonique Commuté, ou à un autre PABX
- les FXS -- Foreign eXchange Station : c'est l'interface reliée au téléphone analogique

pour un FXO :

```
Router(config)# voice-port slot/subunit/port
Router(config-voiceport)# signal groundstart
Router(config-voiceport)# cptone FR
Router(config-voiceport)# station-id name NOM
Router(config-voiceport)# station-id number NUM
```

pour un FXS :

```
Router(config)# voice-port slot/subunit/port
Router(config-voiceport)# signal loopstart
Router(config-voiceport)# cptone FR
Router(config-voiceport)# caller-id enable
Router(config-voiceport)# dial-type dtmf|pulsedialing
```

DTMF est la méthode de numérotation utilisée actuellement

```
Router(config)# show voice port summary
```

Routage intersite Plain Old Telephone Service

```
Router(config)#dial-peer voice NUM pots
Router(config-dial-peer)#destination-pattern NUM
Router(config-dial-peer)#port slot/subunit/port
```

Configuration des lignes numériques

…

ACL = Access List

Une liste de contrôle d'accès ou ACL est un ensemble de règles qui agissent sur les flux entrants ou sortants d'une interface

Ces règles sont parcourues de manière séquentielle

- Lues de haut en bas
- Si correspondance entre la règle et le flux analysé, arrêt de l'analyse
- La dernière règle est une **interdiction implicite**

Actions les plus courantes d'une ACL :

- Filtrage
  * autorisation ou interdiction d'un flux en entrée ou en sortie sur une interface
  * limitation de l'accès à un équipement (administration distante)

- Gestion
  * audit de flux (journalisation)
  * limite l'action d'un protocole (DHCP, NAT, OSPF, BGP)

```
Router#show access-lists          affiche la liste des ACL et leurs statistiques
Router#show ip access-lists       affiche la liste des ACL et leurs statistiques
```

!!! 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 !!! *

liste d'accès standard -> n° d'ACL allant de 1 à 99 et de 1300 à 1999

```
Router(config)#access-list num_ACL permit|deny @SRC @WILDMASK
```

exemples :

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

liste d'accès étendue -> n° d'ACL allant de 100 à 199 et de 2000 à 2699

```
Router(config)#access-list num_ACL permit|deny protocole @SRC @WILDMASK @DST
@WILDMASK eq|lt|gt port [log]

Router(config)#access-list num_ACL permit|deny protocole @SRC @WILDMASK eq|lt|gt port
@DST @WILDMASK [log]
```

exemples :

```
Router(config)#access-list 167 deny udp any any eq 67 log
Router(config)#access-list 168 deny udp any any eq 68 log
pas de bootp depuis tous les RSO vers tous les RSO
Router(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
Router(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
Router(config)#access-list 101 deny ip any any
tout le reste du traffic est interdit
```

liste d'accès standard -> avec un nom

```
Router(config)# ip access-list standard NOM-ACL1
Router(config-ext-nacl)# deny @SRC @WILDMASK
Router(config-ext-nacl)# permit any
```

liste d'accès étendue -> avec un nom

```
Router(config)# ip access-list extended NOM-ACL2
Router(config-ext-nacl)# permit tcp @SRC @WILDMASK gt 1024 host @DST
Router(config-ext-nacl)# permit udp @SRC @WILDMASK host @DST eq tftp
Router(config-ext-nacl)# deny ip any any log
```

exemples d'ACL étendue simulant les règles de filtrage d'un CMAI :

```
Router(config)# ip access-list extended NOM_ACL
Router(config-ext-nacl)#permit tcp host @ROUTEUR_NOIR_côté_CMAI host @CECORE log
TCP du routeur noir vers une station d'admin représentant le CECORE (TCP englobe le SSH)
Router(config-ext-nacl)#permit udp host @REEL_TUN1-loc host @REEL-TUN1_dist eq ISAKMP log
Router(config-ext-nacl)#permit udp host @REEL_TUN2-loc host @REEL-TUN2_dist eq ISAKMP log
ISAKMP du TCE local côté noir vers TCE distants côté noir pour la création des tunnels IPSEC
Router(config-ext-nacl)#permit ospf host @ROUTEUR_NOIR_côté_CMAI host 224.0.0.5 log
Router(config-ext-nacl)#permit ospf host @ROUTEUR_NOIR_côté_CMAI host @CMAI_ROUGE log
OSPF du routeur noir vers le routeur du CMAI
Router(config-ext-nacl)#permit esp @ROUTEUR_NOIR_côté_CMAI @WILDCARDMASK any log
ESP depuis équipement CHIFFRE, à répéter pour chaque équipement
Router(config-ext-nacl)#deny tcp any any log
TCP seulement vers le CECORE
Router(config-ext-nacl)#deny udp any any log
UDP seulement pour les tunnels IPSEC émanant des @TCE_côté_noir
Router(config-ext-nacl)#deny esp any any log
ESP seulement depuis les @TCE_côté_noir
Router(config-ext-nacl)#deny ip any any log-input
tout le reste du traffic est interdit
```

Router(config)# interface type slot/port
Router(config-if)#ip access-group NOM_ACL in|out traffic entrant|sortant
nom d'access-group correspond à nom d' ACL
à appliquer sur le traffic entrant de l'interface côté ROUTEUR NOIR

exemples d'ACL étendue simulant les ACR d'un TCE :

Router(config)# ip access-list extended NOM_ACR1
Router(config-ext-nacl)#permit ip @LAN_loc @WILDCARDMASK @LAN_dist @WILDCARDMASK log
Router(config-ext-nacl)#deny ip any any log
Router(config)# ip access-list extended NOM_ACR2
Router(config-ext-nacl)#permit ip @LAN_loc @WILDCARDMASK @LAN_dist @WILDCARDMASK log
Router(config-ext-nacl)#deny ip any any log

Router(config)# interface tunnel NUM
Router(config-if)#ip access-group NOM_ACR1 ou 2 in|out traffic entrant|sortant
nom d'access-group correspond à nom d' ACR
à appliquer sur le traffic sortant du tunnel souhaité

exemples d'ACL étendue ciblant des champs spécifiques de l'entête TCP :

Router(config)# ip access-list extended CHRISTMAS-TREE
Router(config-ext-nacl)#deny tcp any any match-all +psh +urg +fin log
Router(config-ext-nacl)#permit ip any any
protège des attaques Christmas Tree

liste d'accès dynamique (lock and key)

Permet le passage d'un flux de manière temporaire à travers un routeur si au préalable une authentification via TELNET ou SSH a réussi.
!! Seule une entrée dynamique est possible dans une ACL !!

prérequis :

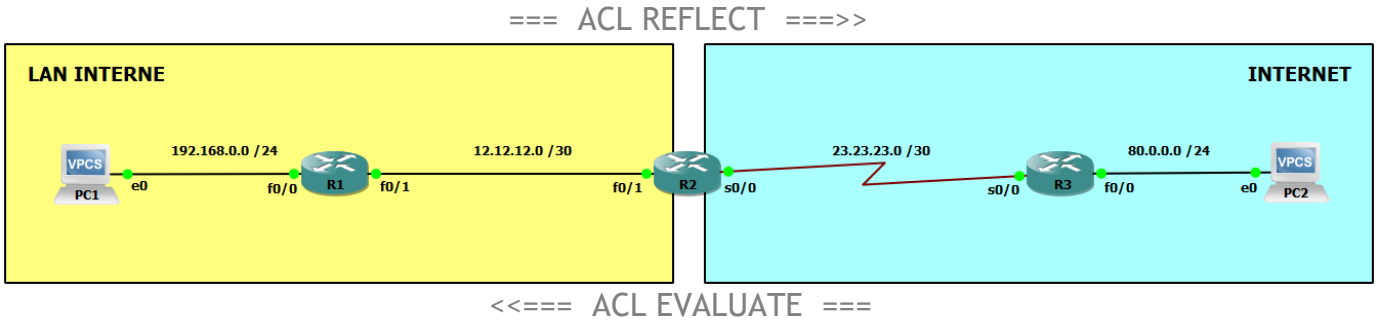
Router(config)#line vty 0
Router(config-line)#autocommand access-enable timeout 5 applicable à un user

Router(config)# ip access-list extended NOM_ACL
Router(config-ext-nacl)#permit tcp host @IP-SRC host @IP-RTR eq telnet | ssh
@IP-SRC = source autorisée à traverser / @IP-RTR = IP utilisée pr joindre le RTR via telnet|ssh
Router(config-ext-nacl)#dynamic NOM_ACL_DYN permit tcp host @IP-SRC host @IP-DST eq www
accès WEB entre les 2 hosts si authentification réussie
Router(config-ext-nacl)#deny ip any any log

CTRL+Z pour retour au mode privilégié

liste d'accès réflexives

Le trafic entrant est permis seulement si une session créée par un flux sortant autorisé a été initiée au préalable. La mise en place de ce mécanisme de filtrage nécessite 2 ACL, une pour les flux sortants, et une pour les flux entrants. Elles s'appliquent à des sessions TCP, UDP et ICMP.




```
Router(config)# ip access-list extended LAN-WAN-REFLECT
Router(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 any reflect WAN-LAN-EVALUATE
Router(config-ext-nacl)#deny ip any any log

Router(config)#  ip access-list extended WAN-LAN-REFLECT
Router(config-ext-nacl)#evaluate WAN-LAN-EVALUATE
Router(config-ext-nacl)#deny ip any any log
```

Appliquer une ACL

```
Router(config)# interface type slot/port
Router(config-if)#ip access-group num_ACL in|out                traffic entrant|sortant
n° d'access-group correspond à n° d' ACL

Router(config)# interface type slot/port
Router(config-if)#ip access-group NOM-ACL1 in|out               traffic entrant|sortant
nom d'access-group correspond à nom d' ACL

Router(config)#line vty 0
Router(config-line)#access-class num_ACL in|out             accès distant entrant|sortant
n° d'access-class correspond à n° d' ACL

Router(config)#line vty  1 4
Router(config-line)#access-class NOM_ACL in|out             accès distant entrant|sortant
nom d'access-class correspond à nom d' ACL
```

QoS= Qualité de Services

Sans QoS, c'est la méthode de base FIFO = First In First Out qui est employée.
C'est le modèle " Best Effort ".

Sélection du flux

Router(config)#class-map match-all|match-any nom_class-map
match-all -> tous les critères doivent correspondre (par défaut)
match-any -> au moins un des critères doit correspondre
Router(config-cmap)#description texte
Router(config-cmap)#match access-group num_ACL ou name nom_ACL
Utiliser une ACL est recommandé pour cibler le traffic auquel appliqué de la QoS
ou
Router(config-cmap)#match destination-address | protocol | ip dscp code | cos | any …
CoS = Class of Services = QoS de niveau 2
Router(config-cmap)#exit

Création des règles de QoS

Router(config)#policy-map nom_policy-map
Router(config-pmap)#class nom_class-map liaison entre policy-map et class-map
Router(config-pmap-c)#set ip dscp code_DSCP
marquage d'un flux dans le champ TOS de l'entête IP avec une valeur EF|AFXX|CSX
EF = Expedited Forwarding | AF = Assured Forwarding | CS = Class Selector
Router(config-pmap-c)#exit

Router(config)#policy-map nom_policy-map
Router(config-pmap)#class nom_class-map liaison entre policy-map et class-map
Router(config-pmap-c)#bandwith kbits/s | bandwith percent % | bandwith remaining percent %
Router(config-pmap-c)#shape adaptative|average bits/sec
Router(config-pmap-c)#priority kbits/sec | priority percent %
Gestion des files d'attente
Router(config-pmap-c)#queue-limit nbre_paquets (64 par défaut)
Router(config-pmap-c)#fair-queue active le Weighted Fair Queuing
Router(config-pmap-c)#random-detect active le Weighted Random Early Detection

Router(config-pmap-c)#police bits/s | police rate bits/s | police cir bits/s bits/sec|%
Router(config-pmap-c-police)#conform-action | exceed-action drop | transmit
Router(config-pmap-c)#exit

Application de la QoS

En mode configuration d'interface
Routeur(config-if)#service-policy input | output nom_policy-map

DNS, service de résolution de noms

Pour l'EAR serveur de noms, déclarer les correspondances NOM et IP :

Router(config)#ip host NOM-1 @IP-1
permet aussi de résoudre les noms en @IP de manière locale sans utiliser de serveur DNS
Router(config)#ip host NOM-2 @IP-2

Router(config)#ip dns server — active le service DNS

Pour l'EAR client DNS :

Router(config)#ip domain lookup
Router(config)#ip name-server @SVR-DNS — possibilité d'en spécifier plusieurs

Activer / Désactiver les fonctionnalités et protocoles inutiles

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

CTRL+Z pour retour au mode privilégié
```

Mode de configuration spécifique

Mode ligne pour les interfaces de connexion au routeur

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

Configurer le port console

```
Router (config)#line console 0
Router(config-line)#logging synchronous                    enlève les affichages perturbateurs
Router(config-line)#exec-timeout minutes secondes
Router(config-line)#login          si authentification simple-> c le password qui est utilisé
Router(config-line)#login local    si authentification locale -> comptes utilisateurs utilisés
Router(config-line)#login authentication default|nom_liste_authentification
si authentification RADIUS -> comptes SAM|AD utilisés
Router(config-line)#password MDP
Router(config-line)#speed BAUD                             9600 par défaut pour CISCO
Router(config-line)#exit
```

Désactiver port auxiliaire

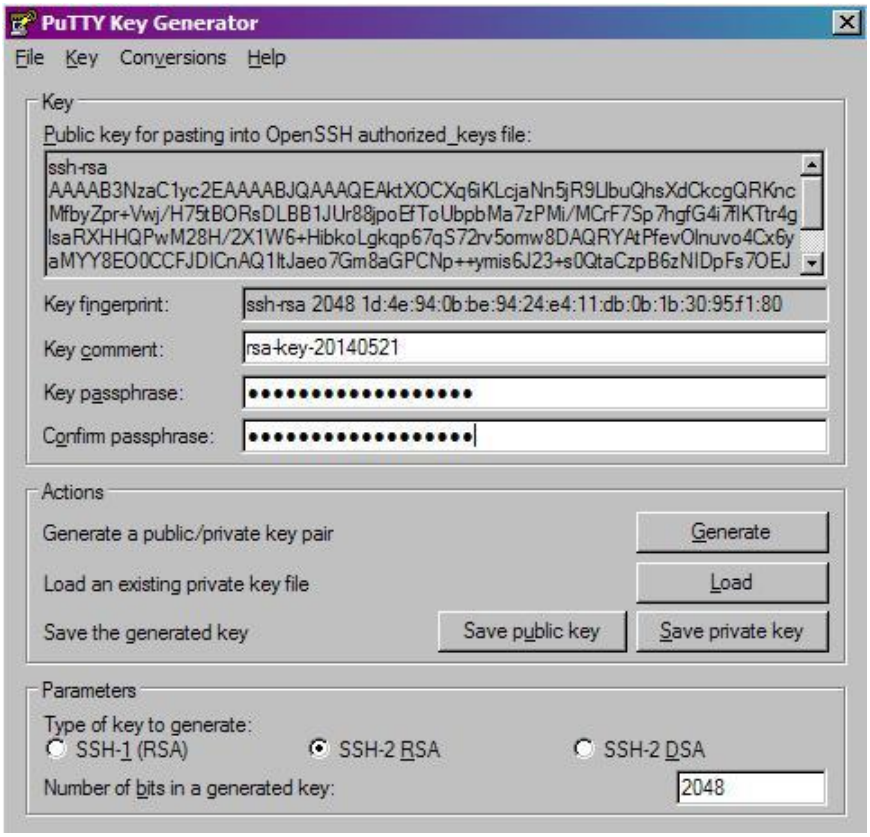
```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#no password
Router(config-line)#no exec
Router(config-line)#exec-timeout 0 1
Router(config-line)#transport input none
Router(config-line)#transport output none
Router(config-line)#transport preferred none
Router(config-line)#exit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

VTY -> TELNET

```
Router(config)#ip telnet source-interface interface slot/port

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

VTY -> SSH = Secure SHell

```
Router(config)#ip ssh version num_version
Router(config)#ip ssh time-out secondes                 temps donné pour se connecter (60 sec)
Router(config)#ip ssh authentication-retries num        mettre 3
Router(config)#ip ssh source-interface interface slot/port
Router(config)#ip ssh logging events                    log des connexions SSH
Router(config)#ip domain-name nom_domaine               exemple -> nom_domaine = NOM_RSO

Router(config)#crypto key generate rsa modulus 2048
      ou
Router(config)#ip ssh pubkey-chain
Router(conf-ssh-pubkey)#username nom_user
c'est la passphrase associée à la clé qui sera demandée lors de la connexion de cet utilisateur
Router(conf-ssh-pubkey-user)#key-string
```



Router(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
Router(conf-ssh-pubkey-data)#exit
Router(conf-ssh-pubkey-user)#exit
Router(conf-ssh-pubkey)#exit

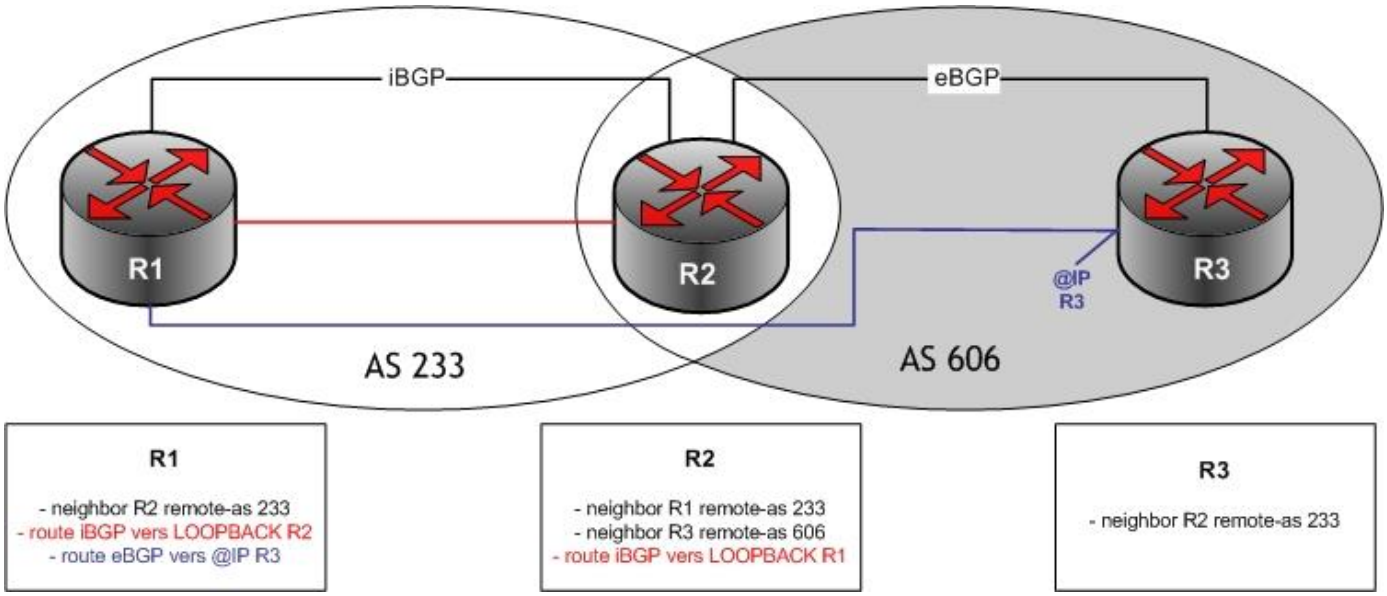
Router(config)#line vty 0 4
Router(config-line)#login si authentification simple-> c le password qui est utilisé
Router(config-line)#login local si authentification locale -> comptes utilisateurs utilisés
Router(config-line)#login authentication default|nom_liste_authentification
si authentification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

Router#show ip ssh affiche l'état et la version du SSH

Mode router pour les protocoles de routage

Router#show ip protocols affiche l'état des protocoles de routage IP

BGP = Border Gateway Protocol



Router(config)#router bgp num_AS
AS = Autonomous System = entité administrative à laquelle appartient le routeur

eBGP

Router(config-router)#neighbor @VOISIN remote-as num_AS AS differente => eBGP
ici le voisin est l'@IP de l'interface connectée au routeur adjacent appartenant à une AS ≠
Router(config-router)#neighbor @VOISIN ebgp-multihop 2 si eBGP avec LOOPBACK

Router(config-router)#router-id @IP @loopback prévue pour iBGP
Router(config-router)#bgp log-neighbor-changes log des upadtes BGP
Router(config-router)#neighbor @VOISIN description EAR

Router(config-router)#neighbor @VOISIN password 0 mdp_en_clair
accès aux updates envoyées par le neighbor en MD5

Router(config-router)#neighbor @VOISIN weight poids
pour influencer le choix de la route à prendre si plusieurs neighbors propage le même RSO
plus le poids est haut (de 0 à 65535) plus les routes du neighbor sont privilégiées
un RSO local à propager à un poids par défaut de 32768
un RSO appris par un neighbor à un poids par défaut de 0
l'attribut weight est propriétaire CISCO

Router(config-router)#neighbor @VOISIN default-originate
envoie une route par défaut au voisin

Router(config-router)#neighbor @VOISIN route-map nom_route-map
affecte les paramètres de propagation et de filtrage des UPDATES BGP (cf. Filtrage BGP)

Router(config-router)#network @RSO mask @masque
l'@RSO et son MASK doit strictement correspondre au réseau connu dans la table de routage
Router(config-router)#network @RSO mask @masque route-map nom_route-map
affecte les paramètres de propagation et de filtrage des UPDATES BGP (cf. Filtrage BGP)

Router(config-router)#redistribute connected optionnel
Router(config-router)#redistribute static si routes statiques à propager
Router(config-router)#redistribute ospf num_process_id
redistribue les réseaux OPSF locaux et ceux appris, dans un autre protocole, ici BGP
Router(config-router)#redistribute ospf num_process_id internal external 1 external 2
redistribue les réseaux OSPF locaux et ceux appris (de type internal, external 1 et 2 = O E1 et O E2), dans BGP à noter que les processus OSPF et BGP doivent exister sur le routeur

Router(config-router)#no synchronization
distribution des réseaux BGP dans l'AS adjacente (eBGP) sans attendre les autres protocoles internes, ici l'OSPF et l'iBGP

Router(config-router)#no auto-summary

iBGP

```
Router(config-router)#neighbor @VOISIN remote-as num_AS          AS identique  => iBGP
ici le voisin est l'@IP de la LOOPBACK BGP du routeur adjacent appartenant à la même AS
Router(config-router)#neighbor @VOISIN update-source loopback num          si neighbor iBGP

Router(config)#ip route @IP-LOOPBACK_iBGP 255.255.255.255 @VOISIN name iBGP
ici @IP de la LOOPBACK BGP est celle du routeur adjacent appartenant à la même AS
sinon, utiliser un IGP (ex:OSPF) entre les RTR iBGP pour apprendre l'@IP-LOOPBACK_iBGP
```

Ici, R1 n'installe pas dans sa table de routage les réseaux annoncés par R3 car il ne connaît pas le nexthop donné avec les routes reçues de R2, les solutions sont :

```
        sur R1
Router(config)#ip route @IP-RSO_eBGP @MASK @VOISIN name eBGP
ici @IP du RSO est celle d'interco R2-R3

        ou sur R2
Router(config-router)#network @IP-RSO_eBGP mask @MASK
ici @IP du RSO est celle d'interco R2-R3

        ou sur R2
Router(config-router)#neighbor @VOISIN next-hop-self
permet d'annoncer les RSO vers le voisin avec sa propre IP en nexthop et non celle d'origine
ici le voisin est l'@IP de la LOOPBACK BGP du routeur adjacent appartenant à la même AS
```

iBGP et Route Reflector

Note: Par défaut, les réseaux appris d'un voisin iBGP ne sont pas annoncés à un autre voisin iBGP. Pour éviter un maillage complet en iBGP, un route reflector est nécessaire :

```
Router(config-router)#neighbor @VOISIN route-reflector-client
```

Peer-group

```
Router(config-router)#neighbor nom_peer-group peer-group
le peer-group permet d'affecter des paramètres communs à tous les membres du groupe
Router(config-router)#neighbor nom_peer-group remote-as num_AS
Router(config-router)#neighbor nom_peer-group update-source loopback num si neighbor iBGP
Router(config-router)#neighbor nom_peer-group password 0 mdp_en_clair
Router(config-router)#neighbor nom_peer-group filter-list in|out          (cf. Filtrage BGP)
Router(config-router)#neighbor nom_peer-group route-map nom_route-map
Router(config-router)#neighbor @VOISIN peer-group nom_peer-group      ajout dans peer-group
```

Filtrage BGP, résumé de routes et modification du routage

Router(config)#route map nom_route-map
Router(config-route-map)#match ip address nom_ACL|num_ACL
Router(config-route-map)#match tag num
Router(config-route-map)#set metric num
Router(config-route-map)#set weight poids
Router(config-route-map)#set local-preference num
l'attribut local-preference (LocPrf) influence le choix de la route apprise si plusieurs neighbors propage le même RSO, plus elle est haute, plus les routes du neighbor sont privilégiées
Router(config-route-map)#set as-path prepend num_AS num_AS
l'attribut as-path (Path) influence le choix de la route apprise si plusieurs neighbors propage le même RSO, moins il y a d'AS traversés, plus les routes du neighbor sont privilégiées
le prepend ajoute des AS traversés lors de l'annnonce faite au voisin, influençant son choix de la meilleure route

!! Attention: ici la route-map agit comme une ACL, elle se finit par un "deny any" implicite !!
Il est nécessaire de permettre tout le reste :
Router(config)#route map nom_route-map permit num_seq

Router(config-router)#neighbor @VOISIN route-map nom_route-map in|out
Router(config-router)#neighbor @VOISIN distribute-list nom_ACL in|out
Router(config-router)#redistribute protocole route-map nom_route-map
Router(config-router)#neighbor @VOISIN prefix-list nom_prefix-list in|out

Router(config)#ip prefix-list nom_prefix-list permit|deny @RSO/MASK

Router(config-router)#aggregate-address @RSO-RESUME @MASK
le @RSO-RESUME et les réseaux incluent dans le résumé sont annoncés
Router(config-router)#aggregate-address @RSO-RESUME @MASK summary-only
seul le @RSO-RESUME est annoncé

Si 2 réseaux sont appris avec un même nombre d'AS traversés, BGP peut installer les 2 dans sa table de routage (de base l'algorithme Best Path Selection ne le permet pas) créant ainsi une répartition de charge via plusieurs neighbors
Router(config-router)#maximum-paths nbre
Router(config-router)#bgp bestpath as-path multipath-relax commande cachée

Fonctions de débug BGP

Router#debug ip bgp events — infos sur les événements BGP

Router#show ip route bgp — affiche la table du protocole de routage BGP

Router#show ip bgp neighbors @IP — affiche le voisinage BGP détaillé
Router#show ip bgp neighbors @IP routes
affiche tous les réseaux appris depuis le voisin
Router#show ip bgp neighbors @IP routes | include XX.XX
filtre l'affichage des RSO appris par le voisin incluant les 2 premiers octets
Router#show ip bgp neighbors @IP advertised-routes
affiche tous les réseaux annoncés au voisin
Router#show ip bgp neighbors @IP received-routes
affiche tous les réseaux appris du voisin si l'inbound soft-reconfiguration est active pour lui

OSPF = Open Shortest Path First

Router(config)#router ospf num_process_id
Router(config-router)#router-id @IP sinon + grande @IP gagne lors de l'activation d'OSPF
Router(config-router)#log-adjacency-changes detail log des maj de la Link State DataBase

Router(config-router)#network @RSO_adjacent @masque_inversé area num_aire
si des NETWORK sont déclarés dans +sieurs aires, alors le routeur est un ABR situé entre l'aire principale de BackBone (l'aire 0) et une autre aire dite secondaire (STANDARD par défaut) par exemple
Attention : une aire secondaire STANDARD peut être connectée à un autre domaine de routage (RIP,BGP..) et peut donc redistribuer les réseaux externes de ce domaine dans le domaine OSPF

Les aires OSPF

Router(config-router)#area num_aire stub à faire sur ABR et IR
une aire secondaire STUB apprends les RSOs des autres aires OSPF (routes O – IA = Inter Area)
les RSOs externes à l'AS ne sont pas appris, ils sont résumés par une route par défaut
Attention : une aire secondaire STUB ne peut pas être connectée à un autre domaine de routage (RIP,BGP) et ne peut donc pas redistribuer les réseaux externes de ce domaine dans le domaine OSPF

Router(config-router)#area num_aire stub no-summary à faire sur ABR et IR
une aire secondaire TOTALLY-STUBBY n'apprends pas les RSOs des autres aires OSPF
les RSOs externes à l'aire et à l'AS ne sont pas appris mais résumés par une route par défaut
Attention : une aire secondaire TOTALLY-STUBBY ne peut pas être connectée à un autre domaine de routage (RIP,BGP) et ne peut donc pas redistribuer les réseaux externes de ce domaine dans le domaine OSPF

Router(config-router)#area num_aire nssa à faire sur ABR et IR
une aire secondaire NOT-SO-STUBBY apprends les RSOs des autres aires OSPF (routes O – IA = Inter Area), les RSOs externes à l'AS ne sont ni appris ni résumés par une route par défaut
Attention : une aire secondaire NOT-SO-STUBBY peut être connectée à un autre domaine de routage (RIP,BGP) et peut donc redistribuer les réseaux externes de ce domaine dans le domaine OSPF

Attention : une aire secondaire STANDARD 1 peut être connectée à une autre aire secondaire STANDARD 2, pour que la 2 connaisse les réseaux extérieurs à la 1 il faut cependant établir un lien virtuel entre l'ABR B situé entre 1 et 2, et l'ABR A situé entre 1 et l'aire backbone 0. Ainsi la 2 se comporte comme si elle était directement connectée à la 0

Router(config-router)#area num_aire_STD2 virtual-link router-id_ABR-A
Router(config-router)#area num_aire_STD1 virtual-link router-id_ABR-B

La redistribution OSPF

Router(config-router)#redistribute connected
Router(config-router)#redistribute static
Router(config-router)#redistribute bgp num_AS
redistribue les réseaux BGP locaux et ceux appris, dans un autre protocole, ici OSPF
à noter que les processus OPSF et BGP doivent exister sur le routeur
Router(config-router)#redistribute protocol metric num
redistribue le protocole voulu dans OSPF en forçant le metric
Router(config-router)#redistribute protocol metric-type 1|2 à faire sur ASBR
redistribue le protocole voulu dans OSPF en changeant le type de route externes (O E1 ou E2)
par défaut routes extérieures au domaine de routage OSPF type E2 et metric = 20
Router(config-router)#redistribute protocol subnets
redistribue le protocole voulu dans OSPF sans tenir compte des classes d'adresse (ClassFull)
prise en compte des adresses CIDR (Classless InterDomain Routing) et donc des sous-réseaux

Router(config-router)#default-information originate
envoie une route par défaut aux routeurs de l'aire connectés en OSPF si une route par défaut est déjà déclarée sur le routeur
Router(config-router)#default-information originate always
envoie une route par défaut aux routeurs de l'aire connectés en OSPF

Optimisation OSPF

Router(config-router)#passive-interface fastethernet|gigabitethernet slot/port
Router(config-router)#prefix-suppression
seuls les réseaux des passive-interface seront annoncés
Router(config-if)#ip ospf prefix-suppression
désactive l'annonce du RSO de cette interface dans OSPF (pas la relation de voisinage)

Router(config-if)#ip ospf network point-to-point
si lien direct et unique entre 2 routeurs (ici CMAI et RTR NOIR)
=> pas délection du DR (Designated Router) et du BDR (Backup DR) pour un lien non série
Pas utile pour un lien série, il est par défaut de type POINT-TO-POINT pour OSPF

Router(config-if)#ip ospf cost valeur modifie le coût du lien OSPF et dc la prorité du chemin
Router(config-if)#bandwith valeur modifie la bande passante, dc le coût et dc la priorité…

Sécurisation OSPF

Router(config-router)#area num_aire authentication message-digest
pour accès à la Link State DB de l'aire en MD5

Router(config)#interface fastethernet slot/port
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf authentication-key mdp
pour authentifier les échanges de routes OSPF sur un lien entre 2 routeurs d'une même aire
ou
Router(config-if)#ip ospf message-digest-key num_clé md5 mdp
pour recevoir les routes OSPF de l'aire dont l'accès est en MD5

Filtrage OSPF et résumé de routes

Router(config-router)#distribute-list nom_ACL in|out

Router(config-router)#area num_aire range @RSO_RESUME @MASK à faire sur ABR
résume les RSOs de l'aire num_aire en un seul RSO, le @RSO_RESUME
Router(config-router)#summary-address @RSO_RESUME @MASK à faire sur ASBR
résume les RSOs externes au domaine OSPF en un seul RSO, le @RSO_RESUME

Fonctions de débug OSPF

Router#debug ip ospf events infos sur les événements OSPF

Router#show ip route ospf affiche la table du protocole de routage OSPF
Router#show ip ospf neighbor affiche le voisinage OSPF détaillé
Router#show ip ospf interface brief affiche les interfaces utilisées par OSPF

RIP = Routing Internet Protocol

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network @RSO_à_déclarer_dans_RIP
Router(config-router)#no auto-summary
désactive les résumés de routes (les @RSO/MASK des réseaux propagés sont conservées)

Router(config-router)#redistribute connected
Router(config-router)#redistribute static
Router(config-router)#redistribute bgp num_AS
redistribue les réseaux BGP locaux et ceux appris, dans un autre protocole, ici RIP
à noter que les processus RIP et BGP doivent exister sur le routeur
Router(config-router)#redistribute protocole metric num
redistribue le protocole voulu dans RIP en forçant le metric ;obligatoire pour RIP et <15
Router(config-router)#redistribute protocole subnets
redistribue le protocole voulu dans RIP sans tenir compte des classes d'adresse (ClassFull)
prise en compte des adresses CIDR (Classless InterDomain Routing) et donc des sous-réseaux

Router(config-router)#passive-interface fastethernet|gigabitethernet slot/port

Router(config-router)#exit
Router(config)#

Fonctions de débug RIP

Router#debug ip rip database infos sur les événements RIP

Mode interface du routeur

Fastethernet, BRI, Loopback

Router(config)#interface loopback num_interface_virtuelle

Router(config)#interface fastethernet slot/port
Router(config)#interface gigabitethernet slot/port

Router(config-if)#media-type sfp, rj45 valable pour les 2900, 3800 et 3900 series
Router(config-if)#no switchport
seulement si le port appartient à une carte switchée et qu'il doit avoir une @IP pour être routé

Router(config-if)#ip address @IP @masque
Router(config-if)#ip address @IP @masque secondary
2°@IP pour un port switché en no switchport /préférer les sous-interfaces pour les ports routés

Router(config-if)#ip address dhcp attribution dynamique d'une @IP par SVR DHCP

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

Router(config-if)#mtu taille_trame définit la taille de la trame ETH

Router(config-if)#ip mtu taille_paquet définit la taille du paquet IP
(ip mtu = mtu max en sortie du chiffreur - 80 octets d'entête (60 IPSEC + 20 trame))

[Router(config-if)#ip tcp adjust-mss taille_segment définit la taille du segment TCP]
(ip tcp adjust-mss = ip mtu - 40 octets d'entête TCP) [optionnel]

Router(config-if)#ip virtual-reassembly réassemblage des fragments d'un même paquet
[Router(config-if)#ip virtual-reassembly max-reassemblies nbre_paquets_réassemblés]
à appliquer seulement si l'EAR atteint son seuil de traitement des paquets fragmentés, par défaut le maximum de fragments traités est de 16 en une fois [optionnel]

Router(config-if)#ip verify unicast rpf non utilisé
Reverse Path Forwarding (s'utilise avec CEF: utile si le routage est symétrique et que le routeur peut vérifier que l'@RSO_SOURCE d'un paquet arrivant par une interface est effectivement accessible par cette interface -> sinon rejet du paquet)

Router(config-if)#ip accounting output-packets
Recense les @IP source et destination et le nombre de paquets vers celles-ci

Router#show ip accounting affiche les @IP_DEST recensées depuis une interface

Router(config-if)#no keepalive
garde actif (UP) le port même si non connecté, désactive les trames de LOOP (protocole de test CISCO d'état des interfaces)
Router(config-if)#keepalive
obligatoire pour une liaison série HDLC/PPP a son propre mécanisme le LCP/préférable pour tout type de liaisons

NETTOYAGE DES INTERFACES

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

Router#show ip interface brief	affiche l'état et l'@IP de toutes les interfaces
Router#show interface description	affiche l'état et la description de toutes les interfaces
Router#show interface status	affiche l'état et le nom de toutes les interfaces

Sous-interfaces

Router(config)#interface gigabitethernet slot/port
Router(config)# media-type sfp, rj45 valable pour les 2900, 3800 et 3900 series
Router(config-if)#speed 10, 100, auto
Router(config-if)#duplex half, full, auto
Router(config-if)#no shutdown
sur les routeurs CISCO toutes les interfaces sont désactivées par défaut
Router(config-if)#exit
Router(config)#

Voir page 43 pour nettoyage de l'interface

Router(config)#interface gigabitethernet slot/port.num_sous_interface
num_sous_interface = ID VLAN
Router(config-if)#encapsulation dot1Q ID VLAN
Router(config-if)# ip address @IP @masque
Router(config-if)#description LAN-SERVEURS_RSO_ZONE
les paramètres de vitesse et de duplex sont déjà définis dans l'interface physique

Voir page 43 pour nettoyage de l'interface

Router(config)#interface gigabitethernet slot/port.num_sous_interface
num_sous_interface = ID VLAN
Router(config-if)#encapsulation dot1Q ID VLAN
Router(config-if)# ip address @IP @masque
Router(config-if)#description LAN-ADMIN_RSO_ZONE
les paramètres de vitesse et de duplex sont déjà définis dans l'interface physique

Voir page 43 pour nettoyage de l'interface

Router(config-if)#no shutdown
sur les routeurs CISCO toutes les interfaces sont désactivées par défaut
Router(config-if)#exit
Router(config)#

Créer un tunnel

Un tunnel sert à encapsuler un protocole dans un protocole de même niveau ou de niveau supérieur. Il permet le traffic entre des réseaux non routés ou non autorisés, ainsi que le passage de protocoles non pris en charge tels que ceux en multicast.

Dans le cas où OSPF est utilisé côté LAN et doit passer à travers les TCE 621, on crée un tunnel sur le routeur ROUGE, car les paquets OSPF en multicast nécessaire pour la màj de la LSDB ne sont pas permis à travers le TCE

```
Router(config)#interface tunnel n°_tunnel
Router(config-if)#description texte
Router(config-if)#ip address @IP_tunnel @masque_tunnel
        ou
Router(config-if)#ip unnumbered fastethernet|gigabitethernet slot/port
```
dans ce cas, assigner une @IP au tunnel n'est pas obligatoire (ex:tunnel traversant un ARKOON)
```
Router(config-if)#tunnel source @IP_int_physique ou nom_interface       côté TCE
Router(config-if)#tunnel destination @IP_int_physique_distante          côté TCE distant
Router(config-if)#tunnel mode ipip ou gre
```
Notes : encapsulation de niv.3 -> GRE par défaut chez CISCO
+ 4 octets d'entête GRE ajouté au paquet IP d'origine (soit 24 octets au total avec l'entête IP supplémentaire rajoutée par le tunnel)
GRE peut transporter des paquets autres que IP
```
Router(config-if)#exit
```

Ensuite il faut déclarer la route statique vers le RSO entre le TCE distant et le routeur ROUGE distant pour que le tunnel soit monté
```
Router(config)#ip route @RSO_distant_TCE_ROUGE @masque @TCE_local_côté_rouge
```

Et déclarer dans OSPF le RSO du tunnel *
```
Router(config)#router ospf num_process_id
Router(config-router)#router-id @IP              @IP = @loopback_prévue_pour_OSPF par ex
Router(config-router)#log-adjacency-changes  log des maj de la Link State DataBase
Router(config-router)#redistribute connected metric 1 subnets      optionnel
Router(config-router)#redistribute static metric 1 subnets         optionnel
Router(config-router)#network @RSO_tunnel @masque_inversé area num_aire

Router(config-router)#exit
Router(config)#
```

Un ping vers l'@IP_tunnel_destination peut être nécessaire pour que le tunnel monte

* Note : Pour supprimer l'annonce des réseaux tunnel dans OSPF
```
Router(config)#interface tunnel n°_tunnel
Router(config-if)#ip ospf prefix-suppression
```

VPN IPSEC

L'IPSEC peut être utilisé pour établir un conduit chiffré entre 2 routeurs faisant ainsi office de chiffreurs.

Cette fonctionnalité repose sur :

-> L'Internet Security Association and Key Management Protocol (ISAKMP) pour associer 2 routeurs
-> L'Internet Key Exchange (IKE) pour l'échange des clés
-> L'Encapsulating Security Payload (ESP) pour garantir l'authentification, l'intégrité et le chiffrement des données du paquet IP et/ou de son entête
-> Authentication Header (AH) pour l'authentification et l'intégrité des paquets

Deux modes de fonctionnement existent pour l'IPSEC :

-> Mode transport = seules les données du paquet IP initial sont chiffrées
-> Mode tunnel = les données et l'entête du paquet IP initial sont chiffrés

Configuration de la phase 1 IPSEC

```
Router(config)#crypto isakmp policy num_policy
définir l'algorithme de chiffrement, ici choisir le plus fort = aes 256
Router(config-isakmp)#encryption des|3des|aes 128|192|256
Router(config-isakmp)#hash sha ou md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 60 à 86400                    en secondes
Router(config-isakmp)#exit

définition du nom de la clé pour le/les routeurs
Router(config)#crypto isakmp key nom_clé address @IP_ROUTEUR2      ex: nom_clé = KVG
Router(config)#crypto isakmp key nom_clé address @IP_ROUTEUR3      ex: nom_clé = KVG
```

Type routeur à routeur (site à site) avec tunnel mode IPSEC

```
Router(config)#crypto ipsec transform-set nom_transform-set esp-aes 256 esp-sha-hmac
ex: nom_transform-set = VPNTCE
Router(cfg-crypto-trans)#mode tunnel|transport
définir le mode tunnel (c'est le mode par défaut chez CISCO)
Router(cfg-crypto-trans)#exit

Création du profil IPSEC
Router(config)#crypto ipsec profile nom_profil          ex: nom_profil = PROFILVPNTCE
Router(ipsec-profile)#set transform-set nom_transform-set
Router(ipsec-profile)#exit
```

Création des 2 tunnels vers les routeurs 1 et 2
Router(config)#interface tunnel n°_tunnel
Router(config-if)#description texte
Router(config-if)#ip address @IP_tunnel @masque_tunnel
Router(config-if)#tunnel source @IP_int_physique ou nom_interface côté TCE NOIR local
Router(config-if)#tunnel destination @IP_ROUTEUR2 côté TCE NOIR distant
Router(config-if)#tunnel mode ipsec ipv4
Router(config-if)#tunnel protection ipsec profile nom_profil

Ensuite il faut déclarer la route statique vers le RSO de la destination du tunnel, ainsi que la ou les routes statiques vers les RSO LAN qui vont passer dans le tunnel.

Du flux doit transiter dans le tunnel pour que le tunnel IPSEC monte.

Type routeur à routeur (site à site) avec crypto-map

Création d'une crypto-map avec ISAKMP
Router(config)#crypto map NOM_CMAP NUM-SEQUENCE ipsec-isakmp
Router(config-crypto-map)#set peer @IP_RTR_distant
Router(config-crypto-map)#set transform-set nom_transform-set
Router(config-crypto-map)#match address nom_ACL ex: nom_ACL = FILTRE_VPN
ACL à utiliser ici devra cibler le trafic entre les LANs transitant dans le VPN IPSEC.
Si utilisation d'un tunnel GRE *, elle devra cibler le traffic GRE entre les @IP SRC et DST du tunnel.
Important : Ici le tunnel GRE est chiffré dans le VPN IPSEC ≠ tunnel mode IPSEC vu avant
Router(config-crypto-map)#exit

Router(config)#interface type slot/port
Router(config-if)#crypto-map nom_CMAP

* pour voir le contenu d'un paquet chiffré et donc le tunnel GRE, et non pas juste de l'ESP, changer le transform-set en AH-SHA-HMAC

Type routeur à routeur (site à site) avec crypto-map sans ISAKMP

Création d'une crypto-map sans ISAKMP
Router(config)#crypto map nom_CMAP 1 ipsec-manual
Router(config-crypto-map)#set peer @IP_RTR_distant
Router(config-crypto-map)#set transform-set nom_transform-set
Router(config-crypto-map)#match address nom_ACL ex: nom_ACL = FILTRE_VPN
Router(config-crypto-map)#set session-key inbound esp SPI cipher 0xhexa authenticator clé
Router(config-crypto-map)#set session-key outbound esp SPI cipher 0xhexa authenticator clé
Les paramètres cipher et authenticator peuvent être identiques sur les 2 RTR
ex : cipher = abcd6789abcd6789
authenticator = 50

Note : inbound du RTR 1 = outbound du RTR 2
outbound du RTR 1 = inbound du RTR 2

Router(config)#interface type slot/port
Router(config-if)#crypto-map nom_CMAP

Type remote-access (clients nomades)

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

Router(config)#aaa authentication login nom_liste_authentification local
ex : nom_liste_authentification = USER_VPN_LOGIN
Router(config)#aaa authorization network nom_liste_authorization local
ex : nom_liste_authorization = USER_VPN_ACCESS

Router(config)#username nom_user secret mdp mdp en MD5

Router(config)#ip local pool nom_pool @IP-DEBUT @IP-FIN
ex : nom_pool = VPN_POOL

Router(config)#crypto isakmp client configuration group nom_grp
ex : nom_grp = VPN_GROUP
Router(config-isakmp-group)#key nom_clé ex : nom_clé = VPN_KEY
Router(config-isakmp-group)#pool nom_pool
Router(config-isakmp-group)#exit

Router(config)#crypto ipsec transform-set nom_transform-set esp-aes 256 esp-sha-hmac
Router(cfg-crypto-trans)#exit ex : nom_transform-set = VPN_RA

Router(config)#crypto ipsec profile nom_profil ex: nom_profil = PROFIL_VPN_RA
Router(ipsec-profile)#set transform-set nom_transform-set
Router(ipsec-profile)#exit

```
Router(config)#interface virtual-template num_VT type tunnel
Router(config-if)#tunnel mode ipsec ipv4
Router(config-if)#tunnel protection ipsec profile nom_profil
Router(config-if)#ip unnumbered fastethernet|gigabitethernet slot/port
Router(config-if)#exit

Router(config)#crypto isakmp profile nom_profil_isakmp
ex : nom_profil_isakmp = PROFIL_ISAKMP_RA
Router(conf-isa-prof)#match identity group nom_grp
Router(conf-isa-prof)#client authentication list nom_liste_authentication
Router(conf-isa-prof)#isakmp authorization list nom_liste_authorization
Router(conf-isa-prof)#client configuration address respond
Router(conf-isa-prof)#virtual-template num_VT
Router(conf-isa-prof)#exit


Router#show crypto session                affiche l'état des sessions IPSEC
```

NAT = Network Address Translation / PAT = Port Address Translation

Possibilité d'utiliser une interface de loopback
Router(config)#interface loopback num_interface_virtuelle
Router(config-if)#description texte
Router(config-if)#ip address @IP_natée @masque
Router(config-if)#exit

Router(config)#interface type slot/port
Router(config-if)#ip address @IP @masque
Router(config-if)#description côté LAN
Router(config-if)#ip nat inside
Router(config-if)#no shutdown

Router(config)#interface type slot/port
Router(config-if)#ip address @IP @masque
Router(config-if)#description côté WAN
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit

Le RSO de NAT doit être routé, si OSPF, ne pas oublier d'annoncer le RSO de NAT
Router(config)#router ospf num_process
Router(config-router)#network @RSO_NAT @masque_inversé area num_aire
Router(config-router)#exit

Router#show ip nat translations affiche la table de traduction du NAT et du PAT

Nater une station (NAT statique)

lien entre l'@IP_réelle et l'@IP_de_NAT
Router(config)#ip nat inside source static @IP_à_nater @IP_natée
ou
Router(config)#ip nat inside source static @IP_à_nater interface type slot/port

Nater un réseau (NAT dynamique)

Router(config)#ip nat pool nom_pool @IP_natée_début @IP_natée_fin netmask @masque
soit le pool contient une plage d'@ prévue pour nater le RSO
soit le pool contient une même @ de début et de fin celle de la loopback

Router(config)#access-list num_ACL permit @RSO_LAN @masque_inversé
Définir une ACL standard permettant de dires quelles @IP du RSO seront natées

Routeur(config)#ip nat inside source list num_ACL pool nom_pool
Lien entre l'ACL et le pool

ou

Routeur(config)#ip nat inside source list num_ACL pool nom_pool overload
overload permet de différencier les machines par un numéro de port car elles utiliseront toutes la même @IP_natée si emploi de l'@ de la loopback dans le pool => PAT

ou

Routeur(config)#ip nat inside source list num_ACL interface type slot/port
Dans ce cas « overload » est appliqué par défaut

Redirection de port

Dans le cas du PAT, si un serveur naté est présent dans le LAN et doit être joint depuis le WAN, ce sera sur des ports spécifiques.

Router(config)# ip nat inside source static tcp|udp @SVR-à-nater port-in @SVR-natée port-out
Ici, extendable sera appliqué par défaut

ou

Router(config)# ip nat inside source static tcp|udp @SVR-à-nater port-in int slot/port port-out

Nater une station (NAT conditionnel)

Note : il n'est pas possible de nater la même @IP en entrée vers deux @IP différentes

```
Router(config)#ip access-list standard LAN-CLIENT
Router(config-std-nacl)#permit @RSO_LAN-CLIENT @masque_inversé
Router(config-std-nacl)#deny any log
Router(config-std-nacl)#exit

Router(config)#route-map NAT_WAN-1
Router(config-route-map)#match ip address LAN-CLIENT
Router(config-route-map)#match interface fastethernet 0/1
Router(config-route-map)#exit

Router(config)#route-map NAT_WAN-2
Router(config-route-map)#match ip address LAN-CLIENT
Router(config-route-map)#match interface fastethernet 1/0
Router(config-route-map)#exit

Router(config)#ip nat inside source route-map NAT_WAN-1 interface fastethernet 0/1 overload
Router(config)#ip nat inside source route-map NAT_WAN-2 interface fastethernet 1/0 overload
```

Les adresses IP du LAN seront natées soit avec l'adresse de f0/1 soit celle de f1/0 selon l'interface de sortie empruntées par les paquets.

BRI = Basic Rate Interface

Router#show isdn status affiche l'état des BRI
Router#show isdn active affiche les appels en cours

Configuration d'une interface physique BRI pour un accès seul

Router(config)#interface BRI slot/port
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#ip address @IP_BRI @masque_BRI
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer map ip @IP_BRI_distante name nom_user broadcast numéro_S0
Le n° de la S0 est celui appelé pour joindre le RSO_BRI distant
Router(config-if)#ppp authentication chap
l'authentification n'est pas obligatoire
Router(config-if)#dialer group num_groupe
n° dialergroup correspond à n° dialerlist
Router(config-if)#dialer idle-timeout secondes
délai d'inactivité après lequel la connexion RNIS / S0 est coupée
Router(config-if)#dialer load-threshold % inbound|outbound|either
% = pourcentage à partir duquel un nouveau canal B est ouvert en entrée / sortie / les 2
Router(config-if)#exit

Router(config)#dialerlist num_groupe protocol ip permit autorise le protocole ip sur la BRI
n° dialerlist correspond à n° dialergroup

Configuration d'une interface physique BRI avec un dialer

```
Router(config)#interface BRI slot/port
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#no ip address
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer rotary-group num_rotary
n° dialer rotary-group correspond à n° interface dialer

Router(config-if)#exit
Router(config)#

Router(config)#interface dialer num_dialer
n° interface dialer correspond à n° dialer rotary-group
Router(config-if)#ip address @IP_BRI @masque_BRI
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer map ip @IP_BRI_distante name nom_user broadcast numéro_S0
Le n° de la S0 est celui appelé pour joindre le RSO_BRI distant
Router(config-if)#ppp authentication chap
l'authentification n'est pas obligatoire
Router(config-if)#dialer-group num_groupe
n° dialergroup correspond à n° dialerlist
Router(config-if)#dialer in-band
le flux de signalisation du canal D passe dans le flux de données des 2 canaux B
Router(config-if)#dialer idle-timeout secondes
délai d'inactivité après lequel la connexion RNIS / S0 est coupée
Router(config-if)#dialer load-threshold % inbound / outbound / either
% = pourcentage à partir duquel un nouveau canal B est ouvert en entrée / sortie / les 2
Router(config-if)#exit

Router(config)#dialerlist num_groupe protocol ip permit   autorise le protocole ip sur la BRI
n° dialerlist correspond à n° dialergroup
```

Configuration de plusieurs interfaces physique BRI avec un dialer (multilink)

```
Router(config)#interface BRI slot/port                    1° BRI physique
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#no ip address
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer rotary-group num_rotary
n° dialer rotary-group correspond à n° interface dialer

Router(config)#interface BRI slot/port                    2° BRI physique
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#no ip address
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer rotary-group num_rotary
n° dialer rotary-group correspond à n° interface dialer

Router(config)#interface BRI slot/port                    3° BRI physique
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#no ip address
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer rotary-group num_rotary
n° dialer rotary-group correspond à n° interface dialer
Router(config-if)#exit
Router(config)#
```

Router(config)#interface dialer num_dialer
n° interface dialer correspond à n° dialer rotary-group
Router(config-if)#ip address @IP_BRI @masque_BRI
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#ppp multilink
Router(config-if)#dialer map ip @IP_BRI_distante name nom_user broadcast numéro_S0
Le n° de la S0 est celui appelé pour joindre la BRI distante
Router(config-if)#ppp authentication chap
l'authentification n'est pas obligatoire
Router(config-if)#dialer-group num_groupe
n° dialergroup correspond à n° dialerlist
Router(config-if)#dialer in-band
le flux de signalisation du canal D passe dans le flux de données des 2 canaux B
Router(config-if)#dialer idle-timeout secondes
délai d'inactivité après lequel la connexion RNIS / S0 est coupée
Router(config-if)#dialer load-threshold 1 either
% = pourcentage à partir duquel un nouveau canal B est ouvert en entrée / sortie / les 2
ici il faut mettre le % à 1 pour ouverture de tous les canaux B en entrée et en sortie
Router(config-if)#exit

Router(config)#dialerlist num_groupe protocol ip permit autorise le protocole ip sur la BRI
n° dialerlist correspond à n° dialergroup

Configuration d'une interface physique BRI avec un dialer string

```
Router(config)#interface BRI slot/port
Router(config-if)#no shutdown
Router(config-if)#isdn switch-type vn3
type de commutateur sur lequel on est raccordé : vn3 -> France
Router(config-if)#no ip address
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer pool-member num_pool
n° dialer pool-member correspond à n° dialer pool

Router(config-if)#exit
Router(config)#

Router(config)#interface dialer num_dialer
Router(config-if)#ip address @IP_BRI @masque_BRI
Router(config-if)#description texte
Router(config-if)#encapsulation ppp
Définit le format de la trame au niveau 2 pour les interfaces Serial ou BRI
Router(config-if)#dialer pool num_pool
n° dialer pool correspond à n° dialer pool-member
Router(config-if)#dialer remote-name nom_routeur
nom du routeur distant
Router(config-if)#dialer string n°S0#
n° de S0 à 7 chiffres
Router(config-if)#dialer idle-timeout secondes
délai d'inactivité après lequel la connexion RNIS / S0 est coupée
Router(config-if)#dialer load-threshold 1 either
% = pourcentage à partir duquel un nouveau canal B est ouvert en entrée / sortie / les 2
ici il faut mettre le % à 1 pour ouverture de tous les canaux B en entrée et en sortie
Router(config-if)#dialer-group num_groupe
n° dialer group correspond à n° dialerlist
Router(config-if)#exit

Router(config)#dialerlist num_groupe protocol ip permit   autorise le protocole ip sur la BRI
n° dialerlist correspond à n° dialergroup
Router(config)#exit
Router#
```

Appeler / Raccrocher un n° S0 avec une interface BRI

```
Router#isdn test call interface bri slot/port numéro_S0
Router#isdn test disconnect interface bri slot/port all / b1 / b2        sélection canal B
```

Fonctions de débug RNIS

```
Router#debug isdn events          infos sur les événements RNIS
Router#debug isdn q921            teste la connexion au commutateur RNIS (niv.2)
Router#debug isdn q931            teste les pb entre routeur et commut RNIS (niv.3)
```

Redondance et liens de secours

VRRP = Virtual Redundancy Router Protocol

Le VRRP est un protocole permettant le couplage de plusieurs équipements physiques afin d'obtenir une redondance de liens pour :

➔ Répartir la charge sur une liaison réseau (passerelles multiples)
➔ Garantir la continuité de services (rapport Maître/Esclave)

La redondance s'etablit par le biais du protocole ARP. Lorsqu'une station doit envoyer une trame à sa passerelle, elle émet une requête ARP et celle-ci répond en fournissant son @MAC.

Dans le cas de VRRP, les routeurs vont associer une @MAC particulière à l'@IP_VIRTUELLE sous la forme **00:00:5E:00:01:XX** (où XX est le num_grp VRRP).
Ce sera cette @MAC qui identifiera la passerelle de la station. De leur côté les routeurs dialoguent par multicast (224.0.0.18) afin de négocier et de savoir qui devra se charger de traiter la trame destinée à l'@MAC VRRP.

Note : Le VRRP bascule automatiquement d'une interface (ROUTEUR MAITRE) à une autre (ROUTEUR ESCLAVE), si les interfaces physiques et virtuelles sont dans le même réseau logique
Cette bascule est transparente et automatique (délai de 3 secs).

à appliquer sur le ROUTEUR MAITRE

Router(config)#interface type slot/port — côté WAN
Router(config-if)#ip address @IP_REELLE_MAITRE @MASQUE — **
Router(config-if)#vrrp num_grp_maître description description
Router(config-if)#vrrp num_grp_maître ip @IP_VIRTUELLE_MAITRE
@IP de l'interface virtuelle du maître
Router(config-if)#vrrp num_grp_maître priority num — exemple -> 200
Indique qui est le maître du groupe « num_grp_maître »
Router(config-if)#vrrp num_grp_esclave description description
Router(config-if)#vrrp num_grp_esclave ip @IP_VIRTUELLE_ESCLAVE
@IP de l'interface virtuelle de l'esclave
Router(config-if)#vrrp num_grp_esclave priority num — exemple -> 100
Indique qui est le maître du groupe « num_grp_esclave »
Router(config-if)#vrrp num_grp_ maître track num_track decrement num — exemple -> 150
Force le maître du groupe « num_grp_maître » à basculer sur l'esclave en baissant sa priorité (ici de 150) selon la règle de track

Router(config)#track num_track interface type slot/port line-protocol
Router(config-track)#delay down secondes
La règle de track s'active seulement si l'interface côté LAN tombe pendant le temps spécifié en secondes

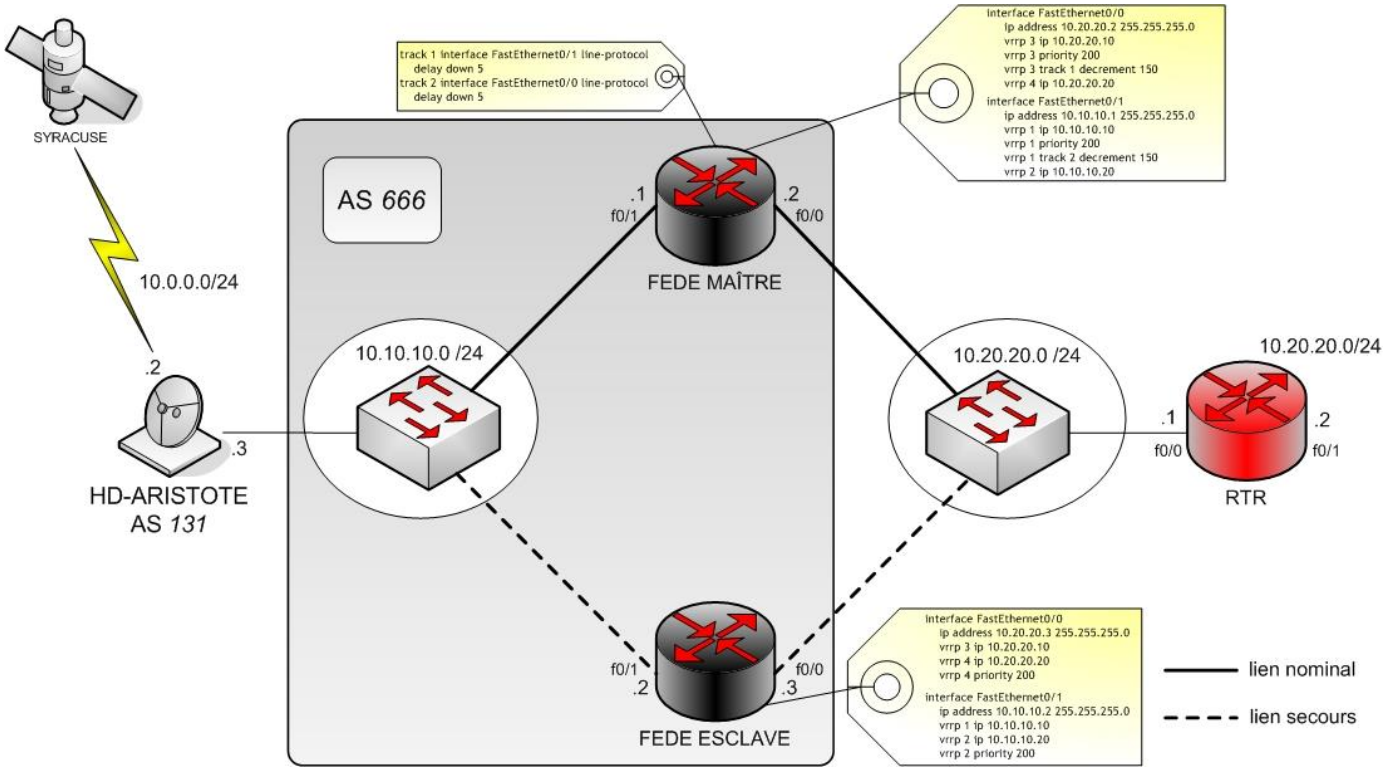
Faire de même pour la configuration VRRP de l'interface côté LAN en y appliquant une règle de track qui s'active seulement si l'interface côté WAN tombe pendant le tps spécifié en secondes

à appliquer sur le ROUTEUR ESCLAVE

Router(config)#interface type slot/port côté WAN
Router(config-if)#ip address @IP_REELLE_ESCLAVE @MASQUE **
Router(config-if)#vrrp num_grp_esclave description description
Router(config-if)#vrrp num_grp_esclave ip @IP_VIRTUELLE_ESCLAVE
@IP de l'interface virtuelle de l'esclave
Router(config-if)#vrrp num_grp_esclave priority num exemple -> 200
Indique qui est le maître du groupe « num_grp_esclave »
Router(config-if)#vrrp num_grp_maître description description
Router(config-if)#vrrp num_grp_maître ip @IP_VIRTUELLE_MAITRE
@IP de l'interface virtuelle du maître
Router(config-if)#vrrp num_grp_maître priority num exemple -> 100
Indique qui est le maître du groupe « num_grp_maître »

Faire de même pour la configuration VRRP de l'interface côté LAN
Pas besoin de règle de track pour l'esclave

Le groupe VRRP num_grp_esclave est inutile sur le ROUTEUR MAITRE et sur le ROUTEUR ESCLAVE, sauf si utilisation de passerelles multiples cf. Note 2



Note 1 : L'@IP à utiliser comme passerelle pour joindre le routeur n'est plus l'@IP_REELLE_MAITRE mais l'@IP_VIRTUELLE_MAITRE

Note 2 : Il n'est utile de spécifier l'@IP_VIRTUELLE_ESCLAVE que lorsqu'on souhaite répartir la charge sur des passerelles multiples (passerelles différentes pour les stations d'un même LAN)

** : VRRP permet d'utiliser directement l'@IP_REELLE, de plus, si utilisation des interfaces physiques pour les @IP des instances VRRP, configurer les priorités devient inutile.
Router(config)#interface type slot/port
Router(config-if)#vrrp num_grp_maître ip @IP_REELLE_MAITRE

Le vrrp preempt est activé par défaut, le premier RTR désigné comme maître du VRRP, même s'il devient esclave lors d'une panne, redeviendra toujours le maître.

Si le preempt est désactivé, le premier RTR désigné comme maître du VRRP, s'il devient esclave lors d'une panne, ne redeviendra pas le maître.
Router(config)#interface type slot/port
Router(config-if)#no vrrp num_instance preempt

HSRP = Hot Standby Router Protocol

Le HSRP est un protocole propriétaire CISCO permettant le couplage de plusieurs équipements physiques afin d'obtenir une redondance de liens pour garantir la continuité de services.

La redondance s'etablit par le biais du protocole ARP. Lorsqu'une station doit envoyer une trame à sa passerelle, elle émet une requête ARP et celle-ci répond en fournissant son @MAC.

Dans le cas de HSRP, les routeurs vont associer une @MAC particulière à l'@IP_VIRTUELLE sous la forme **00:00:0C:07:AC:XX** (où XX est le num_instance HSRP).
Ce sera cette @MAC qui identifiera la passerelle de la station. De leur côté les routeurs dialoguent par multicast (224.0.0.2 en v1 et 224.0.0.102 en v2) afin de négocier et de savoir qui devra se charger de traiter la trame destinée à l'@MAC HSRP.

Note : Le HSRP bascule automatiquement d'une interface (ROUTEUR ACTIF) à une autre (ROUTEUR STANDBY), si les interfaces physiques et virtuelles sont dans le même réseau logique. Cette bascule est transparente et automatique (délai de 3 secs).

Router(config)#interface type slot/port
Router(config-if)#standby num_instance name description
Router(config-if)#standby num_instance ip @IP_VIRTUELLE
Router(config-if)#standby num_instance priority num exemple -> 200
Indique qui est le maître de l'instance, par défaut la priorité = 100
Router(config-if)#standby num_instance preempt

Router(config)#track num_track interface type slot/port line-protocol
Router(config-track)#delay down secondes up secondes
La règle de track s'active seulement si l'interface tombe pendant le temps spécifié en secondes

Router(config)#interface type slot/port
Router(config-if)#standby num_instance track num_track decrement num exemple -> 150
Force le maître de l'instance à basculer sur l'esclave en baissant sa priorité (ici de 150) selon la règle de track

Créer un lien de secours

Router(config)#interface fastethernet slot/port lien principal
Router(config-if)#ip address @IP @masque
Router(config-if)#description texte
Router(config-if)#backup delay secondes_coupure secondes_reprise
secondes_coupure -> tps avant montée de l'interface de secours
secondes_reprise -> tps avant reprise du lien principal
Router(config-if)#backup interface dialer num_dialer
ici le lien de secours est une interface BRI par exemple
Router(config-if)#no shutdown

IP SLAs = Service Levels for IP Applications and services

Router(config)#ip sla monitor NUM_OPERATION

test ECHO-REQUEST
Router(config –ip-sla)#type echo protocol ipIcmpEcho @IP-DST source-ipaddr @IP-SRC
[source-interface type slot/port]
Router(config –ip-sla-echo)#frequency SEC
délai en secondes entre chaque test de l'opération IPSLA
Router(config –ip-sla-echo)#timeout MILLISEC
délai en millisecondes avant que l'opération IPSLA soit considérée en échec
Router(config –ip-sla-echo)#exit

test DNS
Router(config –ip-sla)#type dns target-addr NOM-TEST name-server @IP-SVR-DNS

test de la GIGUE, le port TCP/UDP testé doit être accessible
Router(config –ip-sla)#type jitter dest-ipaddr @IP-DST dest-port 80

test de la VOIP
Router(config –ip-sla)#type jitter dest-ipaddr @IP-DST dest-port NUM codec g711alaw
[advantage-factor 0 à 20]

test TCP | UDP
Router(config –ip-sla)#type tcpConnect dest-ipaddr @DST dest-port NUM [source-port NUM]

Activer la ou les opération(s) IP SLA
Router(config)#ip sla monitor schedule NUM_OP start-time HH:MM:SS|now life sec|forever

Il faut configurer le routeur distant sur lequel le test est fait, si test de la gigue ou VOIP :
Router(config)#ip sla monitor responder

ou si test d'un port spécifique [optionnel]:
Router(config)#ip sla monitor responder type tcpConnect port NUM

Pour envoi de traps vers un serveur SYSLOG
Router(config)#ip sla monitor logging traps active l'envoi de messages SYSLOG
Router(config)#ip sla monitor reaction-configuration NUM_OPERATION react timeout threshold-type immediate action-type trapOnly

Pour envoi de traps vers un serveur SNMP ajouter :
Router(config)#snmp-server enable traps syslog SYSLOG
Router(config)#snmp-server enable traps rtr Response Time Reporter pour IPSLA

Router#sh ip sla monitor configuration
Router#sh ip sla monitor statistics

VRF = Virtual Routing and Forwarding

Le VRF est un procédé permettant de créer plusieurs instances de routage (et donc des tables de routage séparées). Cette séparation des flux offre une notion de sécurité.
Le VRF est similaire aux VLAN :

- 1 switch physique avec x VLAN = x switch virtuels (et x tables de pontage / ARP)
- 1 routeur physique avec y instances VRF = y routeurs virtuels (et y tables de routage)

Router(config)#ip vrf nom_instance

Router(config)#interface nom_interface slot/port
Router(config-if)#ip vrf forwarding nom_instance
assigne l'interface à l'instance de routage VRF définie

Router(config)#router ospf num_process vrf nom_instance
affecte le processus de routage OSPF à l'instance de routage VRF définie

Multicast

Router(config)#ip multicast-routing activation du multicast
Router(config)#interface nom_interface slot/port
Router(config-if)#ip pim sparse-mode
à activer sur toutes les interfaces traversées par des flux multicast
Router(config-if)#exit

Router(config)#ip pim rp-address @IP-RP loopback recommandée
le Rendez-vous Point doit être défini si utilisation du mode clairsemé de PIM (=sparse-mode)

Router(config)#show ip mroute visualiser la table de routage multicast