```
!=========================================
! Configuration VLANs, IP et ACL Sur 5300 XL
!=========================================
conf t
! on active routage IP sur le 5300 XL
     ip routing
! Vlan 1 est utilisé pour manager les switches
    Vlan 1
         ip address 172.16.1.1/24
! configure la fonction relais DHCP
         ip helper-address 10.0.0.5
! Vlan 200 sert à interconnecter les 3 groupes
    vlan 200 name Etab
         untagged A1
         ip address 10.0.0.x/24
         exit
! Vlan 100 est seulement switché sur le 5300 XL, aucun routage
    vlan 100 name admin
         tagged B1
         untagged A2
! Les Vlan 110, 120 et 130 sont routés
    vlan 110 name pedago
        tagged B1
        ip address 172.16.110.1/24
        ip helper-address 10.0.0.5
    vlan 120 name foyer
        tagged B1
        ip address 172.16.120.1/24
        ip helper-address 10.0.0.5
    vlan 130 name visit
        tagged B1
        ip address 172.16.130.1/24
        ip helper-address 10.0.0.5

! Vérification
! liste les ports dans le vlan 1
show vlan 1
! liste les Vlans
show vlan
! liste les ports dans le vlan 110
show vlan 110
! liste à quel Vlan appartient un port donné
show vlan port b1

! liste les adresses IP
show ip
! liste les réseaux IP connus = ici les réseaux « connectés »
show ip route
! liste les réseaux IP connectés
show ip route connected
```

```
! ====================================================
! Réseaux IP distants = routes statiques, RIP, OSPF
!====================================================
! 1 routes statiques
!==================
! Définit les routes statiques vers les autres groupes
    ip route 172.16.0.0/16 10.0.0.1
    ip route 172.17.0.0/16 10.0.0.2
    ip route 172.18.0.0/16 10.0.0.3
show ip route static
! Définit une route par défaut
    ip route 0.0.0.0/0 10.0.0.4

! 2 en RIP
!============
! Active RIP
router rip
! Il faut définir l' interface IP sur laquelle on a des voisins RIP en
RIP
vlan 200
   ip rip

show ip rip
show ip route
show ip route rip

! 3 en OSPF
!============
! Définit un identifiant unique de 32 bits pour le router ospf
ip router-id 10.0.0.1
! Active OSPF
! Area backbone = area 0
router ospf
   area backbone
   exit
! Il faut définir chaque interface IP dans OSPF
vlan 200
   ip ospf area backbone
   exit
vlan 110
   ip ospf area backbone
   exit

vlan 120
   ip ospf area backbone
   exit
vlan 130
   ip ospf area backbone
   exit

! Vérifier
show ip ospf
show ip route
show ip route ospf
```

```
!==============================
! Contrôle d'acces IP = ACL = Access control list
!==============================
! Pour le groupe Admin comme on switche : pas d'ACL
! Pour le groupe ETAB tout le monde peut y accéder

! Definition d'un ACL pour PEDAGO
! L'ACL sera placé en INBOUND (entrant dans le routeur)
conf
ip access-list extended "pedago-control"
! On autorise pedago à accéder au subnet commun ETAB
   permit ip 172.16.110.0/24 172.16.200.0/24
! On autorise pedago à accéder aux subnets Académie maintenanc
   permit ip 172.16.110.0/24 192.168.0.0/16
! On interdit pedago à accéder aux subnets Académie Admin
   deny ip 172.16.110.0/24 10.0.0.0 0.255.255.255
! On interdit pedago à accéder aux autres groupes du lycée
   deny ip 172.16.110.0/24 172.16.0.0/16
! On autorise pedago à accéder au reste = Intranet
   permit ip 172.16.110.0/24 0.0.0.0 255.255.255.255

! Application de l'ACL en inbound
    Vlan 110
        ip access-group pedago-control in

! Definition d'un ACL pour FOYER
ip access-list extended "foyer-control"
! On autorise l'accès au Vlan ETABLISSEMENT (ressources comm)
   permit ip 172.16.120.0/24 172.16.200/24
! On interdit l'accès à l'Intranet
!    172.16/16 = vlans du lycée
    deny ip 172.16.120.0/24 172.16.0.0/12
!    10/8 = Admin Académie
    deny ip 172.16.120.0/24 10.0.0.0/8
!   192.168/16 = Maintenance académie
    deny ip 172.16.120.0/24 192.168.0.0/16
! Le  reste c'est Internet
    permit ip 172.16.120.0/24 any

! Application de l'ACL en inbound
    Vlan 120
        ip access-group foyer-control in


! Exemple de controle d'application
ip access-list extended "appli-control"
! On autorise DNS
     permit udp any any eq dns
     permit tcp any any eq dns
! On autorise http et SSL et c'est tout
     permit tcp any any eq http
     permit tcp any any eq ssl

! attention en utilisant le niveau 4 (TCP ou UDP) on est limité en Bande
passante
```

```
! Pour éditer une ACL
! On la copie dans un éditeur de texte, on l'édite
! On la supprime et on ré-entre toute l'ACL
! Notez que dans la config les /24 sont remplacés par
! 0.0.0.255 = masques inversés ou « wildcard masks »
! et les any par 0.0.0.0 255.255.255.255

no ip access-list extended "foyer-control"
ip access-list extended "foyer-control"
   permit ip 172.16.120.0 0.0.0.255 172.16.200 0.0.0.255
   deny ip 172.16.120.0 0.0.0.255 172.16.0.0/16
   deny ip 172.16.120.0 0.0.0.255 10.0.0.0 0.255.255.255
   deny ip 172.16.120.0 0.0.0.255 192.168.1.0 0.0.0.255
   permit udp 172.16.120.0 0.0.0.255 0.0.0.0 255.255.255.255 eq 53
   permit tcp 172.16.120.0 0.0.0.255 0.0.0.0 255.255.255.255 eq 53
   permit tcp 172.16.120.0 0.0.0.255 0.0.0.0 255.255.255.255 eq 80
   permit tcp 172.16.120.0 0.0.0.255 0.0.0.0 255.255.255.255 eq 443
   permit tcp 172.16.120.0  0.0.0.255 0.0.0.0 255.255.255.255 eq 110
   permit tcp 172.16.120.0  0.0.0.255 0.0.0.0 255.255.255.255 eq 25
   permit tcp 172.16.120.0  0.0.0.255 0.0.0.0 255.255.255.255 eq 585
```