! 1- Config de base

config
! mots de passe locaux
    no password operator
    no password manager
    password manager user-name Sicep21
    password operator user-name Antoine
    show run

! Nom du switch
    hostname RG-BB-254
show cdp neighbors
    console baud-rate 9600
show console

! IP address dans VLAN 1
    vlan 1
        name ETAB
        ip address 172.16.0.254/24
    exit
show ip

show vlan
show vlan 1

! Une bonne méthode = utiliser la commande "setup"
#setup
! permet de configurer SNTP

! 2 Configurer les VLANS et IP
! activer le routage IP
ip routing
! Créer les Vlans, assigner les ports taggés et non taggés et définir l'adresse IP
! L'adresse IP = default gateway pour les PC
! Pour les clients DHCP, activer le relais DHCP
vlan 1
ip add 172.16.0.254
ip helper-address 172.16.0.5
exit
vlan 100 name ADMIN
tagged A1-A4,B1-B4
exit
vlan 110 name PEDAGO
tagged A4
ip address 172.16.110.254/23
ip helper-address 172.16.0.5
exit
vlan 120 name FOYER
tagged A4
ip address 172.16.120.254/23
ip helper-address 172.16.0.5
exit
vlan 130 name GRETA
tagged A4
ip address 172.16.130.254/23
ip helper-address 172.16.0.5
exit
vlan 140 name STI

```
        tagged A4
        ip address 172.16.140.254/23
        ip helper-address 172.16.0.5
    exit
write mem

show ip
show vlan
show vlan 110

! Route statique par défaut
    ip route 0.0.0.0/0 172.16.0.1
show ip route

! Trunk si besoin
    trunk A1-A2 trk1
! tagger un trunk
    vlan 100 tagged trk1
    vlan 110 tagged trk1
    vlan 120 tagged trk1
    vlan 130 tagged trk1
    vlan 140 tagged trk1


! 3 ACCESS_LIST
! Access-list pour VLAN/Subnet PEDAGO
! Interdire l'accès à
FOYER+GRETA+STI+APPLI+VLAN1
! Autoriser l'accès à AD+PROXY/DNS+MAIL
ip access-list PEDAGO1 extended
    deny ip any 172.16.120.0/24
```

```
    deny ip any 172.16.130.0/24
    deny ip any 172.16.140.0/24
    deny ip any 172.16.220.0/24
    deny ip any 172.16.1.0/24
    permit ip 172.16.110.0/23 any

ip access-list PEDAGO2 extended
    permit ip 172.16.110.0/23 172.16.200.0/24
    permit ip 172.16.110.0/23 host 172.16.0.1

ip access-list PEDAGO3 extended
    permit ip 172.16.110.0/23 172.16.200.4/31  permit
ip 172.16.110.0/23 host 172.16.0.1

! Access-list pour VLAN/Subnet FOYER
! Interdire l'accès à
PEDAGO+GRETA+STI+APPLI+VLAN1
! Autoriser l'accès à AD+PROXY-WEB
ip access-list FOYER extended
    permit ip 172.16.110.0/23 172.16.200.4/31  permit
ip 172.16.120.0/24 host 172.16.0.1

! OU Plus simple
! Accès limité au Proxy-web-dns
ip access-list FOYER extended
    permit ip 172.16.120.0/24 host 172.16.0.1


! Access-list pour VLAN/Subnet STI
! Interdire l'accès à
PEDAGO+GRETA+FOYER+VLAN1
```

```
! Autoriser l'accès à AD+APPLI+PROXY-WEB-DNS
ip access-list STI extended

     permit ip 172.16.140.0/24 172.16.220.0/24
     permit ip 172.16.140.0/24 172.16.210.0/24
     permit ip 172.16.140.0/24 172.16.0.1/32

! Access-list pour VLAN/Subnet GRETA
! Interdire l'accès à PEDAGO+STI+FOYER+VLAN1
! Autoriser l'accès à AD+APPLI+PROXY-WEB-DNS
ip access-list STI extended
     permit ip 172.16.140.0/24 172.16.220.0/24
     permit ip 172.16.140.0/24 172.16.210.0/24
     permit ip 172.16.140.0/24 172.16.0.1/32

! Access-list pour VLAN/subnet APPLI
! Interdire l'accès à PEDAGO+FOYER
! Autoriser l'accès à STI+GRETA
ip access-list STI extended
     permit ip 172.16.140.0/24 172.16.220.0/24
     permit ip 172.16.140.0/24 172.16.210.0/24
     permit ip 172.16.140.0/24 172.16.0.1/32

! ACL pour autoriser les flux multicast
ip access-list UTILISATEURS-OUT extended
     permit ip any 224.0.0.0/3
ip access-list SERVEUR-IN extended
     permit ip any 224.0.0.0/3


! Access-list Test
```

```
! Autoriser l'accès à AD+DNS
! Interdire l'intranet
! Autoriser le reste (l'internet)
ip access-list TEST1 extended
     permit ip 172.16.150.0/24 host 172.16.210.5
     permit ip 172.16.150.0/24 host 172.16.210.6
     deny ip any 172.16.0.0/16
     permit ip 172.16.150.0/24 any

ip access-list TEST2 extended
     permit ip 172.16.150.0/24 host 172.16.210.5
     permit ip 172.16.150.0/24 host 172.16.210.6
     permit ip 172.16.150.0/24 host 172.16.0.1


! Access-list pour vlan APPLI en outbound
! Accepte les flux multicast en 239.0.0.0 -
239.255.255.255
! Accepte traffic VLANs utilisateurs STI & GRETA
! Accepte traffc de l'AD + Internet

ip access-list extended APPLI-OUT
     permit ip any 239.0.0.0/24
     permit ip 172.16.130.0/24 any
     permit ip 172.16.140.0/24 any
     permit ip 172.16.210.0/24 any
     deny ip 172.16.0.0/16 any
     permit ip any any


ip access-list extended APPLI-OUT2
```

permit ip 172.16.130.0/24 any
permit ip 172.16.140.0/24 any
permit ip 172.16.210.0/24 any
permit ip host 172.16.0.1 any

! Access-list pour vlan APPLI en inbound
! Autoriser traffic vers VLANs utilisateurs STI & GRETA
! Autoriser traffc vers l'AD + Internet
ip access-list extended APPLI-IN
permit ip 172.16.220.0/24 172.16.130.0/24
permit ip 172.16.220.0/24 172.16.140.0/24
permit ip 172.16.220.0/24 172.16.210.0/24
permit ip 172.16.220.0/24 172.16.0.1/32

! 4 Activer spanning-tree
conf
spanning-tree
! configurer les ports uplinks en non edge
no spanning-tree 25-26 edge-port

! Sur le root et seulement le root (generalement le backbone)
span priority 0

show span
show span config

! Mettre à jour firmware
! Lancer TFTPd32
! Mettre dans dossier du TFTP le firmware
! sur le switch:

#copy tftp flash 172.17.x.y E_10_04.swi secondary

#boot system flash secondary

! Quand ça marche on copie dans la flash première

copy flash flash primary

! 5 MULTICAST

! sur le switch d'accès activer IGMP sur tous les VLANS
Vlan 1
    ip igmp
vlan 110
    ip igmp
vlan 120
    ip igmp
vlan 130
    ip igmp
vlan 140
    ip igmp

! sur le switch backbone activer IGMP sur tous les VLANS

```
Vlan 1
     ip igmp
vlan 110
     ip igmp
vlan 120
     ip igmp
vlan 130
     ip igmp
vlan 140
     ip igmp
vlan 220
     ip igmp
vlan 210
     ip igmp
vlan 200
     ip igmp

! Routage multicast
! Activer Pim sur les interfaces IP (vlans) sur
lesquelles on veut faire passer
! les flux IP multicast
     ip multicast-routing
     router pim
          exit
     vlan 110
          ip pim
     vlan 120
          ip pim
     vlan 130
          ip pim
     vlan 140
```

```
        ip pim
    vlan 220
        ip pim
```

! 6 - Securiser l'acces au switch
! 61 SSH=Secure Shell

```
conf
    cryto key generate ssh
show crypto host-public-key

    ip ssh
    ip ssh key-size 1024
show ip ssh

! utiliser putty côté client


! pour nettoyer la clé
    crypto key zeroize

! quand SSH marche
    no telnet-server
```

!62 SSL = HTTPS

```
! generer la clé publqiue/privée pour SSL
! Générer un cetificat qui contient la clé publique
    crypto key generate cert
    crypto host-cert generate self-signed
! Activer HTTPS
```

web-management ssl
! desactiver le web
no web-management

! 63 IP AUTHORIZED-MANAGERS
! Restreint l'accès à des adresses IP données
conf
ip authorized-managers 172.16.1.0 255.255.255.0
show ip authorized-managers

! 64 SNMP
! Enlever la communauté SNMP "public"
conf
no snmp-server community "public" Unrestricted
show snmp

! Activer SNMP V3
snmp-v3 enable

! 65 Authentifier avec RADIUS
! a- Definir serveur radius
radius-server host 172.16.0.5 key longue-clé-de-20caractères
! Sur le serveurs radius définir les switches comme clients

! b -RADIUS définit le niveau d'accès (login ou enable)
! en retournant l'attribut service-type = Administrative (enable) ou

! NAS-Prompt (login)
aaa authentication login privilege-mode

! c- activer l'authentication Radius pour
! l'accès console, telnet, SSH et Web (inclut ssl)
! Radius est la méthode d'auth. primaire
! si Radius pas accessible on utilise les mots de passe locaux
aaa authentication console login radius local
aaa authentication console enable radius local
aaa authentication telnet login radius local
aaa authentication telnet enable radius local
aaa authentication web login radius local
aaa authentication web enable radius local
aaa authentication ssh login radius local
aaa authentication ssh enable radius local

! 7- QOS
! Sur 2600
! Prioritization par port

conf
    int 1-12
        qos priority 5

! QOS sur 5300
conf
    qos type-of-service diffserv (ou precedence)
! classifier-marquer et prioritiser le traffic du vlan 140 avec un champ diffserv (dscp) au

```
! niveau 3
    vlan 140
        name STI
        qos dscp 001110

! classifier-marquer et prioritiser le traffic TCP 80 pour TOUS les portS avec un champ diffserv (dscp) au niveau 3
    qos tcp-port 80 dscp 001110
```