

Enable
Configure terminal

A) Donnez un nom

hostname SW1

B) Donnez le nom du domaine

ip domain-name ORT

C) Mot de passe secret

enable secret class

banner motd ^CAvez-vous les droits pour vous connecter sur cet appareil^C

D) Mot de passe console

line console 0

password cisco

login

exec-timeout 3 30

logging synchronous

exit

E) Mot de passe vty (pour application Telnet, ssh, putty)

line vty 0 15

password cisco

login

exec-timeout 3 30

logging synchronous

exit

F) Service de cryptage

service password-encryption

G) Adresse IP d'administration

interface vlan 1

description adresse administration distante

ip address 192.168.10.254 255.255.255.0

no shutdown

end

H) Ping d'essai **SUR LUI-MEME**

SW1 # ping 192.168.10.254

Telnet d'essai

SW1 # telnet 192.168.10.254

I) Mettre adresse(s) ip sur les ordinateurs

J) Telnet d'essai distant

```
C:/> telnet 192.168.10.254
```

```
Interface vlan 1
```

```
Description « vlan 1 » non utilisé par la  
suite no ip address
```

```
shutdown  
end
```

Sauvegarde de la configuration courante pour le prochain démarrage

```
SW1 (config-if-range)#do write memory
```

```
SW1 (config-if-range)# end
```

```
SW1 # copy running-config startup-config
```

Building configuration...

[OK]

G°) Déclaration des Vlans

```
Vlan 10
```

```
Name USERS
```

```
Vlan 20
```

```
Name COMPTA
```

```
Vlan 99
```

```
Name ADMIN
```

```
Vlan 66
```

```
Name NATIVE
```

```
Vlan 100
```

```
Name GARAGE
```

G°) Mise en sécurité des ports du commutateur

```
Interface range fastEthernet 0/1-24, GigaEthernet 0/1-2
```

```
Description port dans le garage/Vlan BlackHole
```

```
Switchport access vlan 100
```

```
Shutdown
```

Ceci est aussi possible : **interface range f0/1-4, f0/6-9, f0/11-14, f0/24, g0/1**

H°) Vérification de l'état des ports

Switch# show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual **administratively down down**
FastEthernet0/2 unassigned YES manual administratively down down
FastEthernet0/3 unassigned YES manual administratively down down
FastEthernet0/4 unassigned YES manual administratively down down
FastEthernet0/5 unassigned YES manual administratively down down
FastEthernet0/6 unassigned YES manual administratively down down
FastEthernet0/7 unassigned YES manual administratively down down
FastEthernet0/8 unassigned YES manual administratively down down
FastEthernet0/9 unassigned YES manual administratively down down
FastEthernet0/10 unassigned YES manual administratively down down
FastEthernet0/11 unassigned YES manual administratively down down
FastEthernet0/12 unassigned YES manual administratively down down
FastEthernet0/13 unassigned YES manual administratively down down
FastEthernet0/14 unassigned YES manual administratively down down
FastEthernet0/15 unassigned YES manual administratively down down

FastEthernet0/16 unassigned YES manual administratively down down
FastEthernet0/17 unassigned YES manual administratively down down
FastEthernet0/18 unassigned YES manual administratively down down
FastEthernet0/19 unassigned YES manual administratively down down
FastEthernet0/20 unassigned YES manual administratively down down
FastEthernet0/21 unassigned YES manual administratively down down
FastEthernet0/22 unassigned YES manual administratively down down
FastEthernet0/23 unassigned YES manual administratively down down
FastEthernet0/24 unassigned YES manual administratively down down

GigabitEthernet0/1 unassigned YES manual administratively down down
GigabitEthernet0/2 unassigned YES manual administratively down down
Vlan1 unassigned YES manual administratively down down

I) Vérification de l'état des vlans du port Les ports dans le vlan garage/BlackHole ?

Switch# show vlan

VLAN Name Status Ports

1 default active **doit être vide**

10	USERS	active
20	COMTPA	active
66	NATIVE	active
99	ADMIN	active

100	GARAGE active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
-----	---------------	--

1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

J°) Déclaration des ports en mode Trunk (802.1q)

Interface fastEthernet 0/24

Description lien SW1 vers SW2 en trunk 802.1q

! Si le commutateur accepte ISL et 802.1q faire ci-dessous

```
! switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 10,20,66,99  
switchport trunk native vlan 66
```

```
switchport mode trunk  
switchport nonegotiate  
no shutdown  
  
end
```

Sauvegarde de la configuration courante pour le prochain démarrage

SW1 # copy running-config startup-config

Building configuration...[OK]

K°) Déclaration des ports en mode accès

```
Interface fastEthernet 0/1
  Description port dans le vlan 10
  Switchport mode access
  Switchport access vlan 10
    ! port annuler l'effet spanning-tree
    Spanning-tree portfast
  No shutdown
!
Interface fastEthernet 0/10
  Description port dans le vlan 20
  Switchport mode access
  Switchport access vlan 20
  Spanning-tree portfast
  No shutdown
End

Interface fastEthernet 0/20
  Description port dans le vlan 99 pour admin
  Switchport mode access
  Switchport access vlan 99
  Spanning-tree portfast
  No shutdown
End
```

Vérification :

Switch# show vlan

VLAN Name Status Ports

```
-----
1 default active
10 USERS active
20 COMPTA active
66 NATIVE active
99 ADMIN active
100 GARAGE active
Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17,
Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24,
Gig0/1, Gig0/2

1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
```

ALS2#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/24	on	802.1q	trunking	66

Port Vlans allowed on trunk

Fa0/24 10,20,66,99

Port Vlans allowed and active in management domain

Fa0/24 10,20,66,99

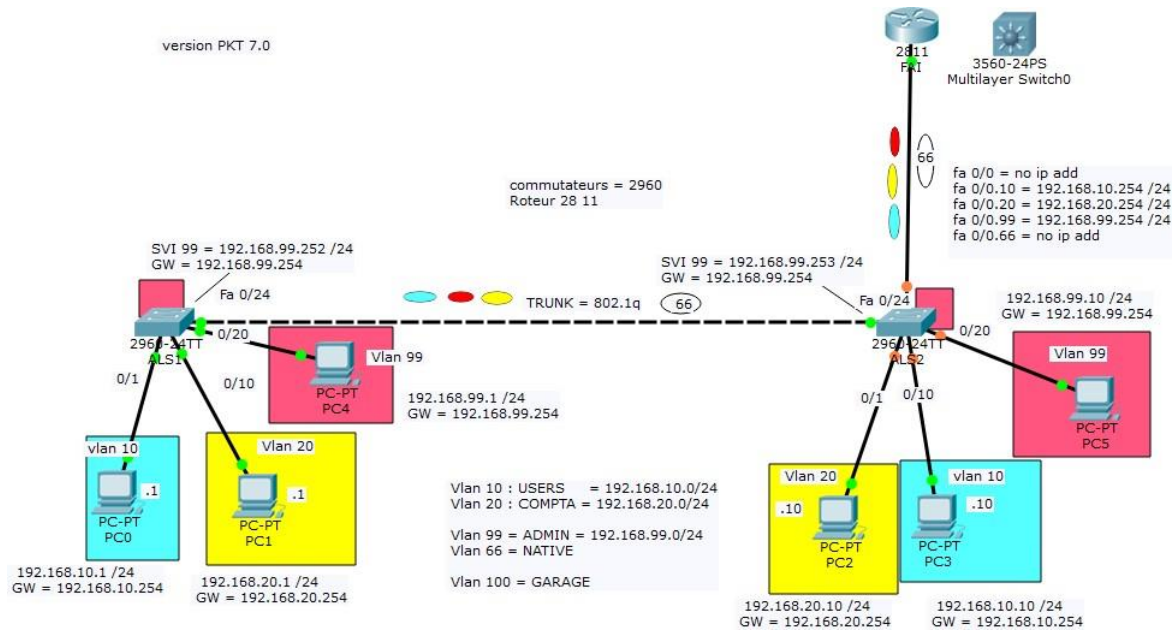
Port Vlans in spanning tree forwarding state and not pruned Fa0/24 none

ALS2#

ALS2#

Changer le protocole spanning-tree

spanning-tree mode rapid-pvst



Insérez la passerelle du commutateur vers l'interface logique du routeur
ip default-gateway 192.168.99.254

Sur l'interface FastEthernet 23

description liaison TRUNK 802.1q entre SW2 et le Routeur
switchport access vlan 100

switchport trunk native vlan 66

switchport trunk allowed vlan
10,20,66,99switchport mode trunk

switchport nonegotiate

Vérification à l'aide de **show interface trunk**

ALS2#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	on	802.1q	trunking	66
Fa0/24	on	802.1q	trunking	66

Sur le routeur (2811)

```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
description vlan users
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0
!
interface FastEthernet0/0.20
description vlan compta
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
!
interface FastEthernet0/0.66
description vlan native
encapsulation dot1Q 66 native
no ip address
```

! Sous interface d'administration

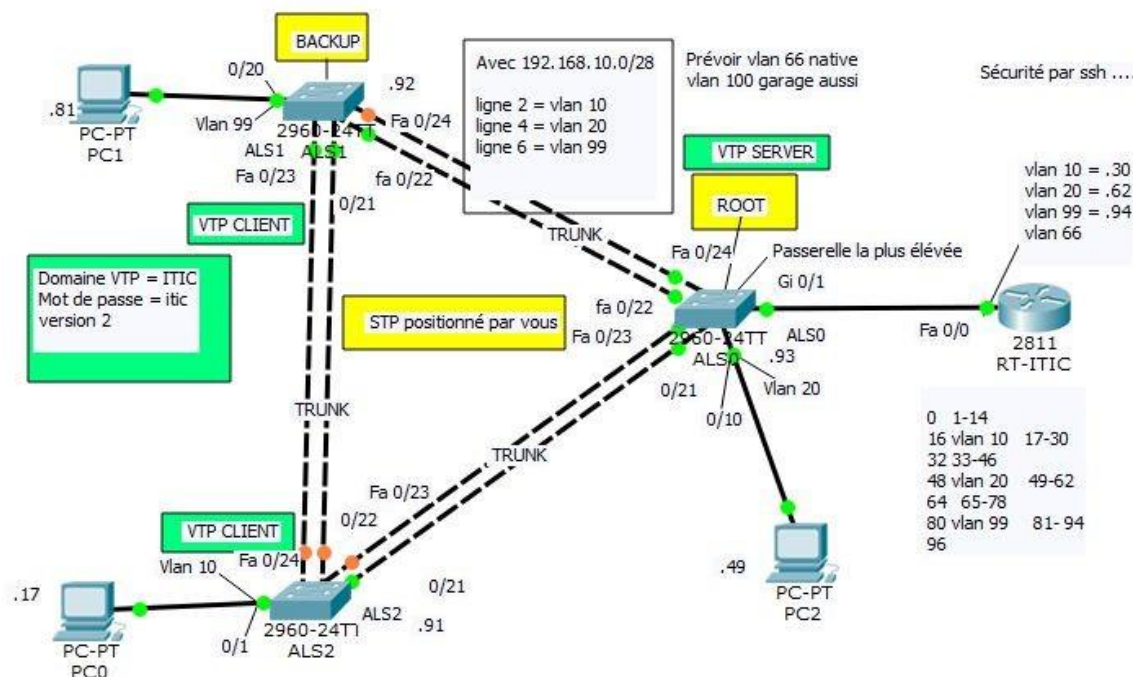
```
interface FastEthernet0/0.99
description vlan admin
encapsulation dot1Q 99
ip address 192.168.99.254 255.255.255.0
no shutdown
```

```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
no shutdown
```

!

Vérification de l'accès aux différents commutateurs et postes via leurs liaisons Trunk

```
Ping 192.168.99.254
Ping 192.168.99.253
Ping 192.168.99.252
Etc....
```



ALS1#sh run

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname ALS1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip domain-name ITIC
!
username patrice secret 5 $1$mERr$suz9Ap3gcgmbTIwvf1FKEz0
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,66,99 priority 28672
!
interface FastEthernet0/1
switchport access vlan 100
shutdown
!
interface FastEthernet0/2
switchport access vlan 100
shutdown
!
interface FastEthernet0/3
switchport access vlan 100
shutdown
```



```
!  
interface FastEthernet0/4  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/5  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/6  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/7  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/8  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/9  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/10  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/11  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/12  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/13  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/14  
switchport access vlan 100  
shutdown  
!
```

```
interface FastEthernet0/15
switchport access vlan 100
shutdown
!
interface FastEthernet0/16
switchport access vlan 100
shutdown
!
interface FastEthernet0/17
switchport access vlan 100
shutdown
!
interface FastEthernet0/18
switchport access vlan 100
shutdown
!
interface FastEthernet0/19
switchport access vlan 100
shutdown
!
interface FastEthernet0/20
description vlan 99
switchport access vlan 99
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/21
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/22
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/23
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
```

```
interface FastEthernet0/24
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
switchport access vlan 100
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 100
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
description vlan 99 SVI
ip address 192.168.10.92 255.255.255.240
!
ip default-gateway 192.168.10.94
!
banner motd ^CAvez-vous les droits pour vous connecter sur cet appareil^C
!
!
!
line con 0
password 7 0822455D0A16
logging synchronous
login
exec-timeout 3 30
!
line vty 0 4
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
!end ALS1#
ALS2#sh run
Building configuration...
```

Current configuration : 3255 bytes

```
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
service password-encryption  
!  
hostname ALS2  
!  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
ip domain-name ITIC  
!  
username patrice secret 5 $1$mERr$uz9Ap3gcgmbTIwvf1FKEz0  
!  
!  
spanning-tree mode rapid-pvst  
!  
interface FastEthernet0/1  
description vlan 10  
switchport access vlan 10  
switchport mode access  
spanning-tree portfast  
!  
interface FastEthernet0/2  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/3  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/4  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/5  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/6  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/7  
switchport access vlan 100  
shutdown
```

```
!  
interface FastEthernet0/8  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/9  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/10  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/11  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/12  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/13  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/14  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/15  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/16  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/17  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/18  
switchport access vlan 100  
shutdown  
!  
interface FastEthernet0/19  
switchport access vlan 100  
shutdown
```

```
interface FastEthernet0/20
switchport access vlan 100
shutdown
!
interface FastEthernet0/21
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/22
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/23
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/24
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
switchport access vlan 100
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 100
shutdown
!
interface Vlan1
no ip address
shutdown
!
```

```
interface Vlan99
description vlan 99 SVI
ip address 192.168.10.91 255.255.255.240
!
ip default-gateway 192.168.10.94
!
banner motd ^CAvez-vous les droits pour vous connecter sur cet appareil^C
!
!
!
line con 0
password 7 0822455D0A16
logging synchronous
login
exec-timeout 3 30
!
line vty 0 4
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
!
!
end
```

ALS2#

ALS0#sh run

Building configuration...

Current configuration : 3448 bytes

!

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname ALS0

!

enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1

!

!

!

ip domain-name ITIC

!

username patrice secret 5 \$1\$mERr\$suz9Ap3gcgmbTIwvf1FKEz0

!

!

spanning-tree mode rapid-pvst

spanning-tree vlan 10,20,66,99 priority 24576

!

interface FastEthernet0/1

switchport access vlan 100

shutdown

!

interface FastEthernet0/2

switchport access vlan 100

shutdown

!

interface FastEthernet0/3

switchport access vlan 100

shutdown

!

interface FastEthernet0/4

switchport access vlan 100

shutdown

!

interface FastEthernet0/5

switchport access vlan 100

shutdown

!

interface FastEthernet0/6

switchport access vlan 100

shutdown

!

interface FastEthernet0/7


```
switchport access vlan 100
shutdown
!
interface FastEthernet0/8
switchport access vlan 100
shutdown
!
interface FastEthernet0/9
switchport access vlan 100
shutdown
!
interface FastEthernet0/10
description vlan 20
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 100
shutdown
!
interface FastEthernet0/12
switchport access vlan 100
shutdown
!
interface FastEthernet0/13
switchport access vlan 100
shutdown
!
interface FastEthernet0/14
switchport access vlan 100
shutdown
!
interface FastEthernet0/15
switchport access vlan 100
shutdown
!
interface FastEthernet0/16
switchport access vlan 100
shutdown
!
interface FastEthernet0/17
switchport access vlan 100
shutdown
!
interface FastEthernet0/18
switchport access vlan 100
shutdown
!
interface FastEthernet0/19
```

```
switchport access vlan 100
shutdown
!
interface FastEthernet0/20
switchport access vlan 100
shutdown
!
interface FastEthernet0/21
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/22
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/23
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/24
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/1
description liaison TRUNK 802.1q
switchport access vlan 100
switchport trunk native vlan 66
switchport trunk allowed vlan 10,20,66,99
switchport mode trunk
switchport nonegotiate
!
```

```
interface GigabitEthernet0/2
switchport access vlan 100
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
description vlan 99 SVI
ip address 192.168.10.93 255.255.255.240
!
ip default-gateway 192.168.10.94
!
banner motd ^CAvez-vous les droits pour vous connecter sur cet appareil^C
!
!
!
line con 0
password 7 0822455D0A16
logging synchronous
login
exec-timeout 3 30
!
line vty 0 4
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
!
!
end
```

ALS0#

Le routeur :

RT-ITIC#sh run

Building configuration...

Current configuration : 1456 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname RT-ITIC

!

enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1

!

ip cef

no ipv6 cef

!

username patrice secret 5 \$1\$mERr\$uz9Ap3gcgmbTIwvf1FKEz0

!

ip domain-name ITIC

!

spanning-tree mode pvst

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

!

interface FastEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.30 255.255.255.240

!

interface FastEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.10.62 255.255.255.240

!

interface FastEthernet0/0.66

encapsulation dot1Q 66 native

no ip address

!

interface FastEthernet0/0.99

encapsulation dot1Q 99

ip address 192.168.10.94 255.255.255.240

!

```
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
banner motd ^CAvez-vous les droits pour vous connecter sur cet appareil^C
!
line con 0
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login
!
line aux 0
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login
!
line vty 0 4
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 3 30
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
!
!
!
end
```

```
RT-ITIC#
RT-ITIC#
```

Voir :

<http://olivier.cochard.me/reseaux/cisco/modele-de-configuration-de-routeur-ios-securisee>

Gestion des logs

! Déclaration du fuseau horaire et du changement d'heure :

clock timezone CET 1 **! Déclaration du fuseau horaire**

clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00 **!**
Heure été/hiver

! Synchronisation NTP de 1'heure :

ntp source-interface loopback0 **! Déclare l'IP de l'interface loopback comme source**

ntp server IP-ADDRESS-NTP-SERVER **! Déclaration du serveur NTP**
ntp authentication key 1 md5 CLEF-NTP **! Déclaration de la clef 1 d'authentification**

ntp trusted-key 1 **! Utilisation de la clef 1**

! Gestion des logs interne :

logging buffered 16384 debugging **! Reserve 16384 octets pour stocker les logs en RAM**

service timestamps debug datetime msec localtime show-timezone **! Marque l'heure/date dans les debug**

service timestamps log datetime msec localtime show-timezone **! Marque l'heure/date dans les logs**

! Gestion de logs centralisé sur un serveur SYSLOG :

logging facility local NUMERO-FACILITY **! Change la facility par défaut (à voir avec le client)**

logging trap

logging IP-ADDRESS-LOG-SERVER **! Adresse IP du serveur Syslog**

service timestamps log datetime msec
service timestamps debug datetime msec
ntp server 192.168.2.10

logging 192.168.2.10

logging trap debugging
ntp update-calendar

Protection juridique

banner login

#Attention !

Acces reserve au personnel du service informatique de NOM-ENTREPRISE.
Toutes activites sur ce systeme sont enregistrees.

Toutes preuves d activites non autorisees seront traitees par les
autoritescompetentes.

Toute intrusion sur un systeme informatique est interdite par les
articles323-1 a 323-7 du Code penal.#

banner motd

#Attention

!

Acces reserve au personnel du service informatique de NOM-ENTREPRISE.
Toutes activites sur ce systeme sont enregistrees.

Toutes preuves d activites non autorisees seront traitees par les
autoritescompetentes.

Toute intrusion sur un systeme informatique est interdite par les
articles323-1 a 323-7 du Code penal.#