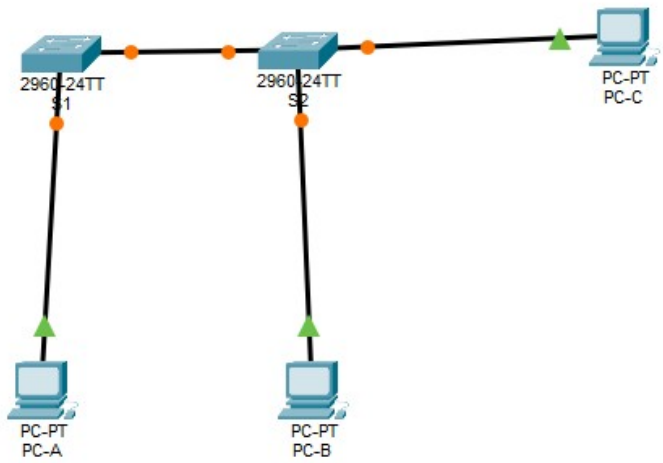
SOMMAIRE

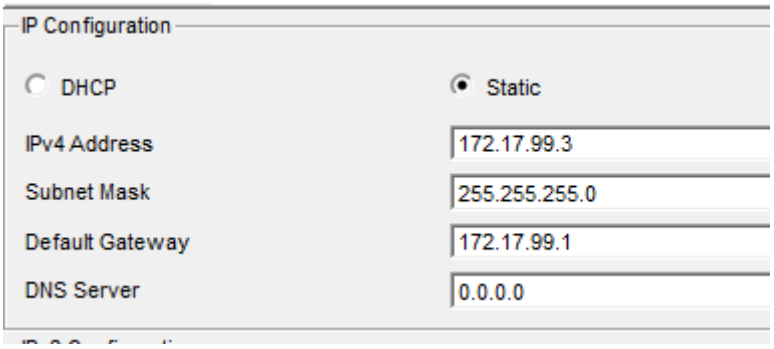
Partie 1 : création du réseau et configuration des paramètres de périphérique de base

Étape 1 : Câblez le réseau conformément à la topologie



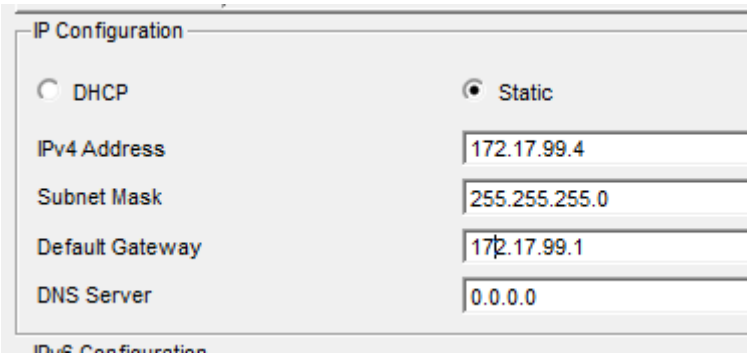
Étape 3 : Configurez les adresses IP sur PC-A, PC-B et PC-C.

PC-A



PC -B

PC-C



Étape 4 : Configurez les paramètres de base pour chaque commutateur.

b. Configurer les noms des périphériques conformément à la topologie.

```
Switch>en
Switch#conf t
Enter configuration com
Switch(config)#host S1
S1(config)#
```

```
Switch>en
Switch#conf t
Enter configuration commands,
Switch(config)#host S2
S2(config)#
```

Étape 5 : Configurez des VLAN sur chaque commutateur.

a. Créer et nommer les VLAN conformément à la table d'attribution des VLAN.

```
S1(config)#vlan 10
S1(config-vlan)#name donnees
S1(config-vlan)#vlan 99
S1(config-vlan)#name management&native
S1(config-vlan)#vlan 999
S1(config-vlan)#Blackhole
                 ^
% Invalid input detected at '^' marker.

S1(config-vlan)#name blackhole
S1(config-vlan)#
```

```
S2(config)#vlan 10
S2(config-vlan)#name donnees
S2(config-vlan)#vlan 99
S2(config-vlan)#name donnees
VLAN #10 and #99 have an identical name: donnees
S2(config-vlan)#name management&native
S2(config-vlan)#name managemant&native
S2(config-vlan)#vlan 999
S2(config-vlan)#name Blackhole
S2(config-vlan)#
```

b. Configurez l'adresse IP indiquée dans la table d'adressage de VLAN 99 sur les deux commutateurs.

```
Enter configuration commands, one per line
S1(config)#int vl 1
S1(config-if)#no ip addres
S1(config-if)#no ip address
S1(config-if)#int vl 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed
ip address 172.17.99.11 255.255.255.0
S1(config-if)#
```

```
S2(config)#int vlan 1
S2(config-if)#no ip  add
S2(config-if)#no ip  address
S2(config-if)#int vl 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
ip add
S2(config-if)#ip address
% Incomplete command.
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#
```

```
S1(config)#int f0/6
S1(config-if)#switch mode access
S1(config-if)#switch access vlan 99
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on
```

c. Configurez F0/6 sur S1 en tant que port d'accès et attribuez-le à VLAN 99.

d. Configurer F0/11 sur S2 en tant que port d'accès et attribuez-le à VLAN 10 et Configurez F0/18 sur S2 en tant que port d'accès et attribuez-le à VLAN 99.

```
Enter configuration commands, one per lin
S2(config)#int f0/11
S2(config-if)#switchpor mode a
S2(config-if)#switchpor mode access
S2(config-if)#switch ac
S2(config-if)#switch access vlan 10
S2(config-if)#int f0/18
S2(config-if)#switchpor mode access
S2(config-if)#switch access vlan 99
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Inte
```

f. Exécuter la commande **show vlan brief** afin de contrôler les attributions de VLAN et de ports

```
sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- --------
1    default                           active    Fa0/1, F
                                                 Fa0/5, F
                                                 Fa0/10,
                                                 Fa0/14,
                                                 Fa0/18,
                                                 Fa0/22,
                                                 Gig0/2
10   donnees                           active
99   management&native                 active    Fa0/6
999  blackhole                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

```
S2#
%SYS-5-CONFIG_I: Configured from console by console
sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- --------
1    default                           active    Fa0/1, F
                                                 Fa0/5, F
                                                 Fa0/9, F
                                                 Fa0/14,
                                                 Fa0/19,
                                                 Fa0/23,
10   donnees                           active    Fa0/11
99   Blackhole                         active    Fa0/18
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#sh vl br

VLAN Name                              Status    Ports
```

À quel VLAN un port non attribué, tel que F0/8 sur S2, appartiendrait-il ?
Tous les ports par défaut sont attribués à VLAN 1.

Étape 6 : Configurez la sécurité de base du commutateur.

c. Désactiver tous les ports physiques non utilisés.

```
S1(config)#int rang f0/2-5
S1(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/2,

%LINK-5-CHANGED: Interface FastEthernet0/3,

%LINK-5-CHANGED: Interface FastEthernet0/4,

%LINK-5-CHANGED: Interface FastEthernet0/5,
S1(config-if-range)#int rang f0/7-24
S1(config-if-range)#shut
```

```
S1(config)#int rang g0/1-2
S1(config-if-range)#shut
```

```
S2(config)#int rang f0/2-10
S2(config-if-range)#shut

2(config-if-range)#int rang f0/12-17
2(config-if-range)#shut

int rang f0/19-24
S2(config-if-range)#shut
```

Étape 7 : Vérifiez la connectivité entre les périphériques ainsi que les informations VLAN.

a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse de gestion de S1. Les requêtes ping ont-elles abouti ? Pourquoi ?

Oui, les requêtes ping ont abouti. PC-A est dans le même VLAN que l'adresse de gestion sur le commutateur.

```
Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
```

b. À partir de S1, envoyez une requête ping à l'adresse de gestion de S2. Les requêtes ping ont-elles abouti ? Pourquoi ?

Non, les requêtes ping ont échoué. Les adresses de gestion sur S1 et S2 se trouvent dans le même VLAN, mais l'interface F0/1 sur les deux commutateurs n'est pas configurée en tant que port trunk. Le port F0/1 appartient toujours au VLAN 1 et non au VLAN 99.

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

c. À partir d'une invite de commande sur PC-B, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A et PC-C. Les requêtes ping ont-elles abouti ? Pourquoi ?

Les requêtes ping vers S1, S2, PC-A et PC-C à partir de PC-B n'avaient pas abouti. PC-B est dans le VLAN 10, et S1, S2, PC-A et PC-C dans le VLAN 99. Il n'y a aucun périphérique de couche 3 à router entre les réseaux.

```
C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

d. À partir d'une invite de commande sur PC-C, envoyez une requête ping aux adresses de gestion sur S1 et S2. Avez-vous réussi ? Pourquoi ?

Réussite partielle. PC-C est dans le même VLAN que S1 et S2. PC-C peut envoyer une requête ping à l'adresse de gestion de S2, mais ne peut toujours pas envoyer de requête ping vers S1, car aucune liaison trunk n'a été établie entre S1 et S2.

```
Pinging 172.17.99.12 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Partie 2 : implémentation de la sécurité VLAN sur les commutateurs

Étape 1 : Configurez les ports trunk sur S1 et S2.

a. Configurez le port F0/1 de S1 en tant que port trunk.

```
S1(config)#int f0/1
S1(config-if)#switch mode trunk
```

b. Configurez le port F0/1 de S2 en tant que port trunk.

```
S2(config)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#
```

c. Vérifiez le trunking sur S1 et S2. Exécutez la commande **show interface trunk** sur les deux commutateurs.

```
S1#
%SYS-5-CONFIG_I: Configured from console by console
sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Étape 2 : Modifiez le VLAN natif pour les ports trunk de S1 et S2.

La modification du VLAN natif pour les ports trunk à partir du VLAN 1 vers un autre VLAN est une méthode de sécurité recommandée.

a. Quel est le VLAN natif actuel pour les interfaces F0/1 de S1 et S2 ?

Le VLAN 1 est le VLAN natif des deux commutateurs.

b. Configurez le VLAN natif sur l'interface trunk F0/1 de S1 à VLAN 99 - Management&Native.

```
Enter configuration commands, one per lin
S1(config)#swicth
S1(config)#swict
S1(config)#swic
S1(config)#swic
S1(config)#int f0/1
S1(config-if)#swit trunk native vlan 99
S1(config-if)#sw
S1(config-if)#
```

c. Attender quelques secondes. Vous devriez commencer à recevoir des messages d'erreur dans la session en mode console de S1. Que signifie le message « %CDP-4-NATIVE_VLAN_MISMATCH: » ?

Il s'agit d'un message de Cisco Discovery Protocol (CDP) indiquant que les VLAN natifs de S1 et S2 ne correspondent pas. Le VLAN

d. Configurez le VLAN natif sur l'interface trunk F0/1 de S2 à VLAN 99.

```
S2(config)#int f0/1
S2(config-if)#sw trun native vl 99
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0099.
Port consistency restored.
```

e. Vérifiez que le VLAN natif est désormais le VLAN 99 sur les deux commutateurs. Le résultat de S1 est affiché ci-dessous.

```
S2#
%SYS-5-CONFIG_I: Configured from console by console
sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99
```

```
S1#
%SYS-5-CONFIG_I: Configured from console by console
sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Étape 3 : Vérifiez que le trafic peut correctement traverser la liaison trunk.

a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse de gestion de S1. Les requêtes ping ont-elles abouti ? Pourquoi ?
Oui, les requêtes ping ont abouti. PC-A est dans le même VLAN que l'adresse de gestion sur le commutateur.

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time=3ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
```

b. À partir de la session en mode console sur S1, envoyez une requête ping à l'adresse de gestion de S2. Les requêtes ping ont-elles abouti ? Pourquoi ?

Oui, les requêtes ping ont abouti. Le trunking a été établi avec succès et les deux commutateurs se trouvent dans le VLAN 99.

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

c. À partir d'une invite de commande sur PC-B, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A et PC-C. Les requêtes ping ont-elles abouti ? Pourquoi ?

Les requêtes ping vers S1, S2, PC-A et PC-C à partir de PC-B n'avaient pas abouti. PC-B est sur le VLAN 10, tandis que S1, S2, PC-A et PC-C sont sur le VLAN 99. Il n'y a aucun périphérique de couche 3 à router entre les réseaux.

```
Control-C
^C
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.

Ping statistics for 172.17.99.11:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

Request timed out.

Ping statistics for 172.17.99.3:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 172.17.99.4

Pinging 172.17.99.4 with 32 bytes of data:

Request timed out.

Ping statistics for 172.17.99.4:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

d. À partir d'une invite de commande sur PC-C, envoyez une requête ping aux adresses de gestion sur S1 et S2, et à l'adresse IP de PC-A. Avez-vous réussi ? Pourquoi ?

Les requêtes ping ont toutes abouti. PC-C est dans le même VLAN que S1, S2 et PC-A.

```
C:\>ping 172.17.99.11

Pinging 172.17.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255
Reply from 172.17.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255
Reply from 172.17.99.12: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Étape 4 : Empêchez l'utilisation du protocole DTP sur S1 et S2.

Vous pouvez observer ce comportement par défaut en exécutant la commande suivante :

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management&native)
Voice VLAN: none
```

a. Désactivez la négociation sur S1.

```
S1(config)#int f0/1
S1(config-if)#swit
S1(config-if)#switchport nego
S1(config-if)#switchport no n
S1(config-if)#switchport none
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

b. Désactivez la négociation sur S2.

```
S2(config)#int f0/1
S2(config-if)#switch nonego
S2(config-if)#switch nonegotiate
```

c. Vérifiez que la négociation est désactivée en exécutant la commande **show interface f0/1 switchport** sur S1 et S2.

```
S1#sh int f0/1 switc
S1#sh int f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management&native)
```

Étape 5 : Sécurisez les ports d'accès sur S1 et S2.

.

a. Exécutez la commande **show interface f0/2 switchport** sur S1. Notez le mode d'administration et l'état de la négociation de trunking.

```
S1#
S1#sh int f0/2 swit
S1#sh int f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

b. Désactiver le trunking sur les ports d'accès de S1.

```
S1(config)#int rang f0/2-5
S1(config-if-range)#switchport mode access
S1(config-if-range)#sw access vlan 999
S1(config-if-range)#
```

c. Désactiver le trunking sur les ports d'accès de S2.

```
S2(config-if)#int rang f0/2-5
S2(config-if-range)#sw mod acc
S2(config-if-range)#sw mod access
S2(config-if-range)#sw acce vl 999
```

d. Vérifier que le port F0/2 est configuré pour accéder à S1.

```
sh int f0/2 sw
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 999 (blackhole)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

e. Vérifiez que les attributions des ports VLAN sur les deux commutateurs sont correctes. S1 est indiqué ci-dessous à titre d'exemple.

```
S1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
10   donnees                           active
99   management&native                 active    Fa0/6
999  blackhole                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

f. Faire en sorte que le port trunk F0/1 sur S1 n'autorise que les VLAN 10 et 99.

```
S1(config)#int f0/1
S1(config-if)#sw trunk all
S1(config-if)#sw trunk allowed vlan 10,99
S1(config-if)#
```

g. Faire en sorte que le port trunk F0/1 sur S2 n'autorise que les VLAN 10 et 99.

```
S2(config)#int f0/1
S2(config-if)#sw trunk allowed vlan 10,99
S2(config-if)#
```

h. Vérifier les VLAN autorisés. Exécutez une commande **show interface trunk** en mode d'exécution privilégié à la fois sur S1 et S2.

```
S1#
%SYS-5-CONFIG_I: Configured from console by console
sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99

S1#
```

```
S2#
%SYS-5-CONFIG_I: Configured from console by console
sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

Quel est le résultat ?
Seuls les VLAN 10 et 99 sont autorisés sur la liaison trunk entre S1 et S2.

Quels sont, le cas échéant, les problèmes de sécurité liés à la configuration par défaut d'un commutateur Cisco ?

Le fait que tous les ports soient attribués par défaut à VLAN 1 est un problème de sécurité potentiel. Un autre problème est que, sur de nombreux commutateurs Cisco, le trunking est défini à la négociation automatique, et par conséquent il se peut que les liaisons trunk soient activées à votre insu lors de la connexion d'un commutateur non autorisé. Une autre réponse possible est que les mots de passe de console et vty sont affichés par défaut en texte clair. Par ailleurs, le serveur HTTP est activé par défaut.