# Configurer l'accès convergent dans un réseau de petite filiale à commutateur unique

## Contenu



## Introduction

Ce document fournit des exemples de configuration pour le déploiement de l'accès convergent dans un réseau de commutateurs de petite filiale unique. Ces configurations peuvent être utilisées dans des centaines voire des milliers de filiales pour déployer le réseau sans fil dans les filiales avec des configurations testées et éprouvées.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur de la gamme Catalyst 3850
- Cisco IOS version 03.03.00SE ou ultérieure
- Cisco IES version 1.2 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

# Informations générales

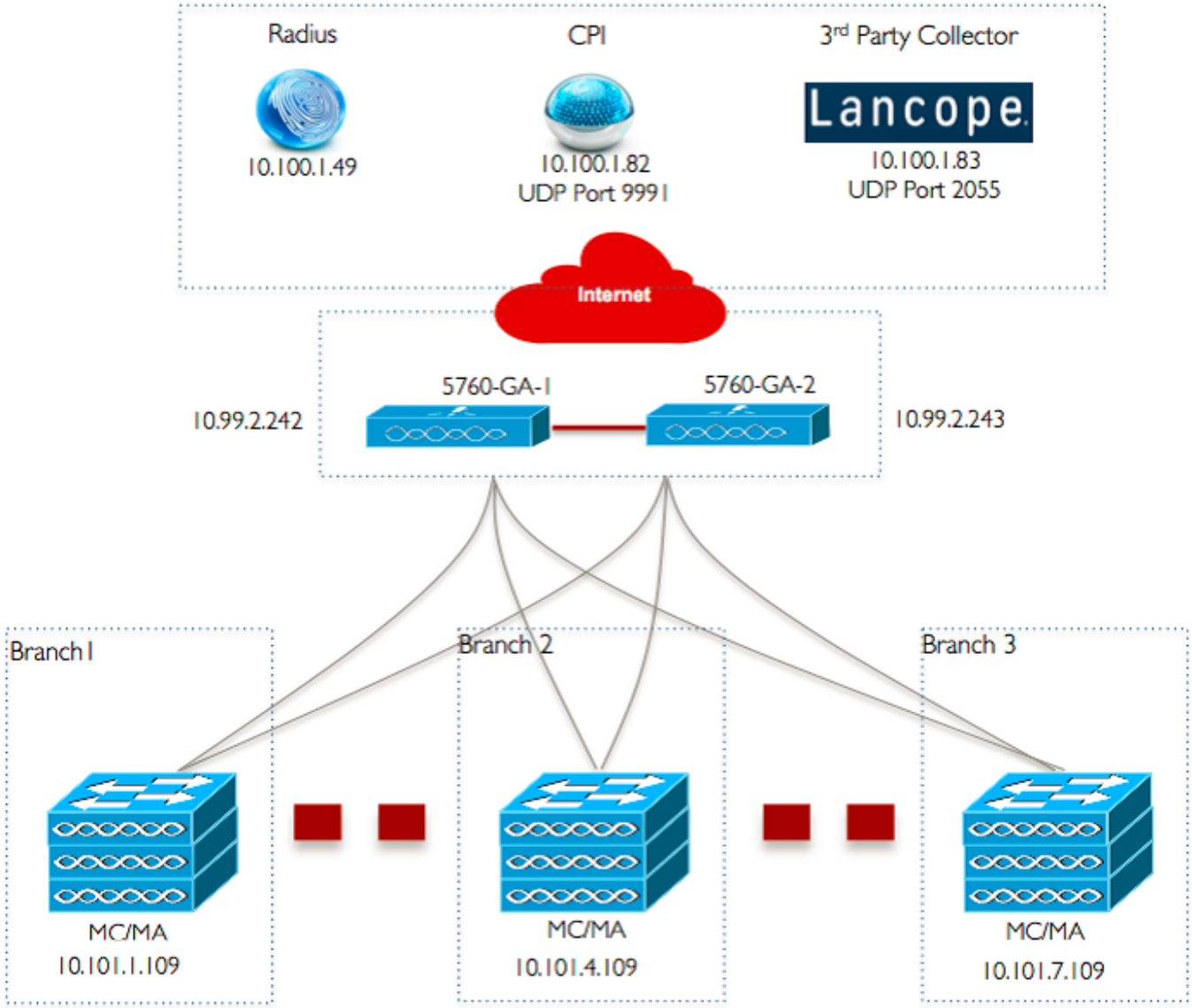
La petite succursale distante ou le magasin de détail peut se composer d'une seule ou d'une pile de commutateurs Ethernet pour fournir une connectivité réseau aux utilisateurs filaires et sans fil. De tels petits réseaux peuvent faire converger la commutation Ethernet avec une fonctionnalité sans fil nouvelle génération sur le même commutateur Catalyst.

Pour de telles conceptions de réseau, le commutateur peut intégrer des fonctions de contrôleur de mobilité et d'agent de mobilité (MA) du contrôleur de réseau local sans fil (WLC) sans nécessiter d'éléments d'accès convergent supplémentaires, tels que le groupe d'homologues de commutateur (SPG) dans le réseau. Ces réseaux peuvent nécessiter des services sans fil invités, ainsi que l'application commune des politiques de sécurité et d'accès réseau dans toutes les filiales.

# Configuration

## Diagramme du réseau

Cette image illustre une topologie de référence pour un réseau de succursale type.




## Configurations

### Configuration de la couche 2/3 de base

- **Mode VTP (VLAN Trunk Protocol) : Transparence**

Cet exemple montre la configuration du mode VTP.

```
vtp domain ‘name'
vtp mode transparent
```

- **Spanning Tree: Rapid-Per VLAN Spanning Tree (PVST)**

Cet exemple montre la configuration Rapid-PVST.

```
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
spanning-tree extend system-id
```

- **Créer des VLAN nommés**

Cet exemple montre comment les VLAN sont créés.

```
vlan 151
name Voice_VLAN
!
vlan 152
name Video_VLAN
!
vlan 155
 name WM_VLAN
!
vlan 158
name 8021X_WiFi_VLAN
```

- **Configurer la passerelle par défaut**

La configuration de la passerelle par défaut est présentée dans cet exemple.

```
ip default-gateway <ip address>
ip route vrf Mgmt-vrf 0.0.0.0 0.0.0.0 172.26.150.1
```

- **Configurer le routage et le transfert virtuels de gestion (VRF)**

La configuration VRF de gestion est présentée dans cet exemple.

```
interface GigabitEthernet0/0
description Connected to FlashNet - DO NOT ROUTE
vrf forwarding Mgmt-vrf
ip address 172.26.150.202 255.255.255.0
no ip redirects
no ip proxy-arp
load-interval 30
carrier-delay msec 0
negotiation auto
no cdp enable

vrf definition Mgmt-vrf
```

- **Configuration de la surveillance DHCP IP**

Dans cet exemple, la surveillance DHCP est configurée pour tous les VLAN client sans fil.

```
ip dhcp snooping vlan 151-154,156-165
no ip dhcp snooping information option
ip dhcp snooping wireless bootp-broadcast enable
ip dhcp snooping
```

> **Note**: Les ports de liaison ascendante doivent être marqués comme des ports de confiance, comme indiqué dans l'exemple de ports de liaison ascendante/Port-Channel.

- **Configurer l'inspection ARP (Address Resolution Protocol)**

Dans cet exemple, l'inspection ARP est configurée pour tous les VLAN client sans fil.

```
ip arp inspection vlan 151-154,156-165
ip arp inspection validate src-mac dst-mac ip allow zeros
```

> **Note**: Les ports de liaison ascendante doivent être marqués comme des ports de confiance, comme indiqué dans l'exemple de ports de liaison ascendante/Port-Channel.

- **Ports de liaison ascendante/Port-Channel (autoriser les VLAN nécessaires)**

Dans cet exemple, le port de liaison ascendante/Port-Channel est configuré.

```
interface Port-channel1
description Connected Dist-1
 switchport trunk native vlan 4002
switchport trunk allowed vlan 151-166,4093
switchport mode trunk
 ip arp inspection trust
load-interval 30
carrier-delay msec 0
 ip dhcp snooping trust


interface GigabitEthernet1/1/1
description Connected Dist-1
switchport trunk native vlan 4002
switchport trunk allowed vlan 151-166,4093
switchport mode trunk
ip arp inspection trust
load-interval 30
channel-protocol pagp
channel-group 1 mode desirable
ip dhcp snooping trust

interface GigabitEthernet1/1/2
description Connected Dist-1
switchport trunk native vlan 4002
switchport trunk allowed vlan 151-166,4093
switchport mode trunk
 ip arp inspection trust
load-interval 30
 channel-protocol pagp
channel-group 1 mode desirable
 ip dhcp snooping trust
```

## Mobilité

- **Interface de gestion sans fil**

Dans cet exemple, la fonctionnalité sans fil est activée et le WLC 5760 Guest Anchor est configuré comme homologue de mobilité.

```
interface vlan 105
description Wireless Management Interface
```

```
 ip address 10.101.1.109 255.255.255.240
load-interval 30
logging event link-status
no shutdown

wireless management interface vlan 105

wireless mobility group name 3850_Branch_1
wireless mobility group member ip 10.99.2.242 public-ip 10.99.2.242 group GA-Domain-1
wireless mobility group member ip 10.99.2.243 public-ip 10.99.2.243 group GA-Domain-2
```

**Remarque** : vous pouvez utiliser un WLC Cisco 5508 ou un AireOS 8510 comme contrôleur d'ancrage invité.

## Sécurité

- **Paramètres globaux**

Cet exemple montre la configuration des paramètres globaux.

```
       aaa new-model
aaa authentication login PRIME_RADIUS_AUTH_GRP group PRIME_RADIUS_SERVER_GRP
aaa authentication dot1x PRIME_RADIUS_AUTH_GRP group PRIME_RADIUS_SERVER_GRP
aaa authorization network PRIME_RADIUS_AUTHO_GRP group PRIME_RADIUS_SERVER_GRP
aaa authorization network PRIME_CWA_MAC_FILTER group PRIME_RADIUS_SERVER_GRP
aaa accounting Identity PRIME_RADIUS_ACCT_GRP start-stop group PRIME_RADIUS_SERVER_GRP


aaa server radius dynamic-author
client 10.100.1.49 server-key 7 02050D480809
 auth-type any
!
!
radius server PRIME_RADIUS_SERVER_1
address ipv4 10.100.1.49 auth-port 1812 acct-port 1813
timeout 1

key 7 121A0C041104
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 31 send nas-port-detail
!
aaa group server radius PRIME_RADIUS_SERVER_GRP
server name PRIME_RADIUS_SERVER_1
```

## WLAN

- **WLAN 802.1X**

La configuration WLAN 802.1X est présentée dans cet exemple.

```
wlan ABCCorp-8021X 1 ABCCorp-8021X
```

```
band-select
aaa-override
nac
wifidirect policy deny
client vlan 8021X_WiFi_VLAN
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
accounting-list PRIME_RADIUS_ACCT_GRP
security dot1x authentication-list PRIME_RADIUS_AUTH_GRP
session-timeout 21600
wmm require
no shutdown
```

- WLAN à clé prépartagée

La configuration du WLAN à clé prépartagée est présentée dans cet exemple.

```
wlan ABCCorp_PSK 2 ABCCorp_PSK
band-select
client vlan PSK_WiFi_VLAN
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
no security wpa akm dot1x
security wpa akm psk set-key ascii 8 AAPAAQeRgFGCE_dLbEOcNPP[AAAAAAMcLKMPc^TcSbIhbU\HeaSXF_AAB
service-policy output ABCCorp_PSK-PARENT-POLICY
session-timeout 7200
wifidirect policy deny
wmm require
no shutdown
```

- Ouvrir WLAN

La configuration Open WLAN est présentée dans cet exemple.

```
wlan ABCCorp_OPEN 3 ABCCorp_OPEN
band-select
client vlan Open_WiFi_VLAN
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
no security wpano security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy output ABCCorp_OPEN-PARENT-POLICY
session-timeout 1800
wifidirect policy deny
wmm require
no shutdown
```

## Solution invité

- WLAN invité CWA

La configuration WLAN invité CWA est présentée dans cet exemple.

```
wlan ABCCorp-Guest 15 ABCCorp-Guest
aaa-override
accounting-list PRIME_RADIUS_ACCT_GRP
client vlan GUEST_VLAN
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
```

```
load-balance
security dot1x authentication-list PRIME_RADIUS_AUTH_GR
Pmac-filtering PRIME_CWA_MAC_FILTER
mobility anchor 10.99.2.242
mobility anchor 10.99.2.243
nac
no security wpa
no security wpa am dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
session-timeout 3600
wmm require
no shutdown
```

- Configuration WLAN de mobilité et d'invité sur 5760 Guest Anchor 1

Dans cet exemple, Mobility and Guest WLAN est configuré sur 5760 Guest Anchor 1.

```
wireless mobility group name GA-Domain-1
wireless mobility group member ip 10.101.1.109 public-ip 10.101.1.109 group 3850_Branch_1

wlan ABCCorp-Guest 15 ABCCorp-Guest
aaa-override
accounting-list PRIME_RADIUS_ACCT_GRP
client vlan GUEST_WiFi_VLAN
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
load-balance
security dot1x authentication-list PRIME_RADIUS_AUTH_GRP
mac-filtering PRIME_CWA_MAC_FILTER
mobility anchor 10.99.2.242
nac
no security wpa
no security wpa am dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
session-timeout 3600
wmm require
no shutdown
```

- Redirection de la liste de contrôle d'accès pour CWA (authentification Web centrale)

La configuration pour rediriger l'ACL pour CWA est présentée dans cet exemple.

```
Extended IP access list PRIME-CWA-REDIRECT-ACL
10 deny icmp any any
20 deny udp any eq bootps any
30 deny udp any any eq bootpc
40 deny udp any eq bootpc any
50 deny udp any any eq domain
60 deny tcp any any eq domain
70 deny ip any host 10.100.1.49
80 permit tcp any any eq www
```

## Services sans fil IOS avancés

- Configuration de la visibilité et du contrôle des applications (AVC)

Cet exemple montre la configuration d'AVC.

```
flow exporter PRIME_FNF_COLLECTOR_1
description FLEXIBLE NETFLOW COLLECTOR
```

```
destination 10.100.1.82
dscp 46
transport udp 9991
!
!
flow monitor wireless-avc-basic
exporter PRIME_FNF_COLLECTOR_1
record wireless avc basic
```

- **Configuration WLAN**

Cet exemple montre la configuration du WLAN.

```
wlan ABCCorp-8021X 1 ABCCorp-8021X
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
```

- **Mise en forme de la bande passante de sortie pour les WLAN**

L'exemple illustre la configuration du formatage de la bande passante de sortie pour les WLAN.

```
policy-map ABCCrop-8021X-PARENT-POLICY
description PRIME-ABCCorp-8021X EGRESS PARENT POLICY
class class-default
shape average percent 40
queue-buffers ratio 0

policy-map ABCCorp-PSK-PARENT-Policy
description PRIME-ABCCorp-PSK EGRESS PARENT POLICY
class class-default
shape average percent 30
queue-buffers ratio 0
```

- **Configuration WLAN**

Cet exemple montre la configuration du WLAN.

```
wlan ABCCorp-8021X 1 ABCCorp-8021X
service-policy output ABCCorp-8021X-PARENT-POLICY
```

## Meilleures pratiques

Les meilleures pratiques en matière de configuration sans fil sont les suivantes :

- Utilisation de la commande **wireless client fast-ssid-change** pour configurer la modification rapide du SSID.
- Utilisation des commandes **passwd encryption on** and **passwd key obfuscate** pour le cryptage de mot de passe.