Configurez Access convergé dans un petit réseau de branchement de Simple-commutateur

Contenu

Introduction

Ce document fournit des configurations d'échantillon pour le déploiement Converged Access dans un réseau commuté simple de petite taille-branchement. Ces configurations peuvent être utilisées à travers des centaines ou même des milliers de branchements pour déployer le réseau Sans fil aux filiales avec - et - des configurations testées éprouvées.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Commutateur de gamme Catalyst 3850
- Version 03.03.00SE ou ultérieures de Cisco IOS
- Version 1.2 ou ultérieures IES de Cisco

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

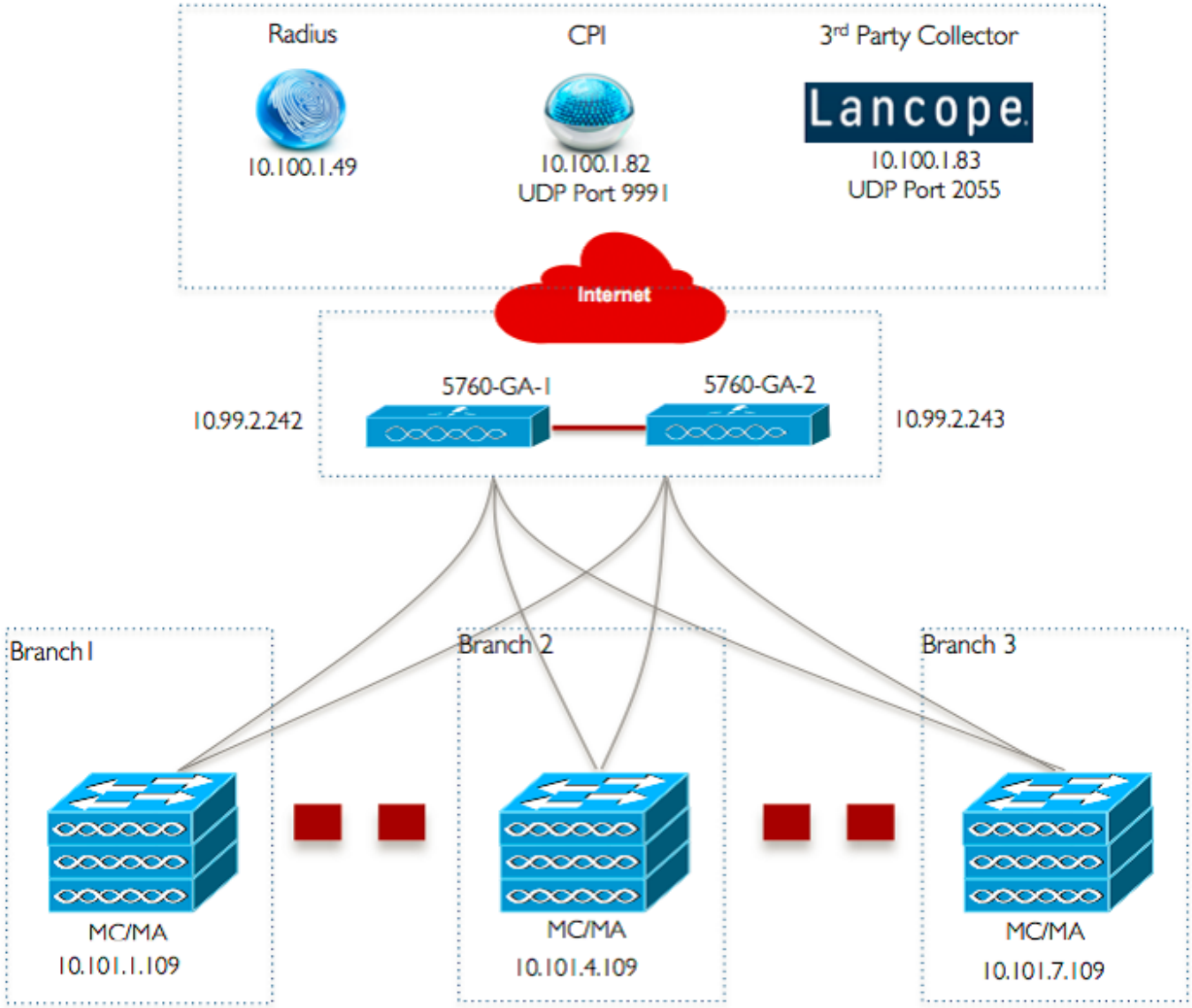
La succursale distante ou le commerce de détail de petite taille peut se composer d'un simple ou d'une pile de commutateurs ethernets pour fournir la connexion réseau au câbler et aux utilisateurs de sans fil. De tels petits réseaux peuvent converger la commutation d'Ethernets avec la fonctionnalité sans fil de la deuxième génération sur le même commutateur de Catalyst.

Pour de telles conceptions de réseaux, le commutateur peut intégrer des fonctions Sans fil de contrôleur de mobilité du contrôleur LAN (WLC) et d'agent de mobilité (mA) sans n'exiger aucun élément convergé supplémentaire d'Access, tel que le Commutateur-Pair-groupe (SPG) dans le réseau. Ces réseaux peuvent exiger des Services sans fil d'invité, aussi bien que l'application de Sécurité commune et de stratégie d'accès au réseau à travers toutes les succursales.

Configurez

Diagramme du réseau

Cette image illustre une topologie de référence pour un réseau de branchement typique.



Configurations

Configuration de la couche de base 2/3

- **Mode de protocole VTP (VLAN Trunk Protocol) : Transparent**

Cet exemple affiche la configuration du mode VTP.

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

- **Spanning-tree : Rapide-par spanning-tree VLAN (PVST)**

Cet exemple affiche la configuration rapide-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
```

- Create a nommé des VLAN

Cet exemple affiche 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
```

- Configurez la passerelle par défaut

La configuration de passerelle par défaut est affichée 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
```

- Configurez le Virtual Routing and Forwarding de Gestion (le VRF)

La configuration de VRF de Gestion est affichée 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
```

- Configurez l'ip dhcp snooping

Dans cet exemple, la surveillance DHCP est configurée pour tout le client sans fil VLAN.

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

> Remarque: Des ports uplinks doivent être marqués comme confiance suivant les indications de l'exemple de ports uplinks/Port canalisé.

- Configurez l'inspection de Protocole ARP (Address Resolution Protocol)

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

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

Remarque: Des ports uplinks doivent être marqués comme confiance suivant les indications de l'exemple de ports uplinks/Port canalisé.

- **Ports uplinks/Port canalisé (permettez les VLAN nécessaires)**

Dans cet exemple, le port uplink/Port canalisé 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 l'ancre WLC de 5760 invités est configurée en tant que pair 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 Cisco 5508 WLC ou des 8510 AireOS comme contrôleur d'ancre d'invité.

Sécurité

- **Paramètres globaux**

Cet exemple affiche 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

- **802.1X WLAN**

La configuration du 802.1X WLAN est affichée 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
```

- **Clé pré-partagée WLAN**

La configuration pré-partagée de la clé WLAN est affichée 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
```

- Ouvrez le WLAN

La configuration ouverte WLAN est affichée 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 d'invité

- Invité WLAN CWA

La configuration de l'invité WLAN CWA est affichée 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 de mobilité et d'invité WLAN sur l'ancre 1 de 5760 invités

Dans cet exemple, la mobilité et l'invité WLAN est configurée sur l'ancre 1. de 5760 invités.

```
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
```

- Réorientez l'ACL pour CWA (le Web-Auth central)

La configuration pour réorienter l'ACL pour CWA est affichée 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 avancés IOS

- Visibilité d'application et configuration du contrôle (AVC)

Cet exemple affiche 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 affiche la configuration du WLAN.

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

- Bande passante de sortie formant pour des WLAN

L'exemple affiche la configuration de la bande passante de sortie formant pour des 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 affiche la configuration du WLAN.

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

Meilleures pratiques

Les pratiques recommandées pour la configuration Sans fil incluent :

- Utilisant la commande de rapide-SSID-**modification de client sans fil** de configurer changer rapide SSID.
- Utilisant le **cryptage de passwd en fonction** et la **clé de passwd assombrissez les** commandes pour le cryptage de mot de passe.