

La configuración convergió acceso en una pequeña red derivada del un solo switch

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Movilidad](#)

[Seguridad](#)

[red inalámbrica \(WLAN\)](#)

[Solución del invitado](#)

[Servicios inalámbricos avanzados IOS](#)

[Mejores medidas](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento proporciona las configuraciones de muestra para el despliegue convergido del acceso en una red del un solo switch de la pequeño-bifurcación. Estas configuraciones se pueden utilizar a través de los centenares o aún de los millares de bifurcaciones para desplegar la red inalámbrica en las redes derivadas con - y - las configuraciones probadas probadas.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 3850 Series Switch
- Versión deL Cisco IOS 03.03.00SE o más adelante
- Versión 1.2 o posterior de Cisco IES

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

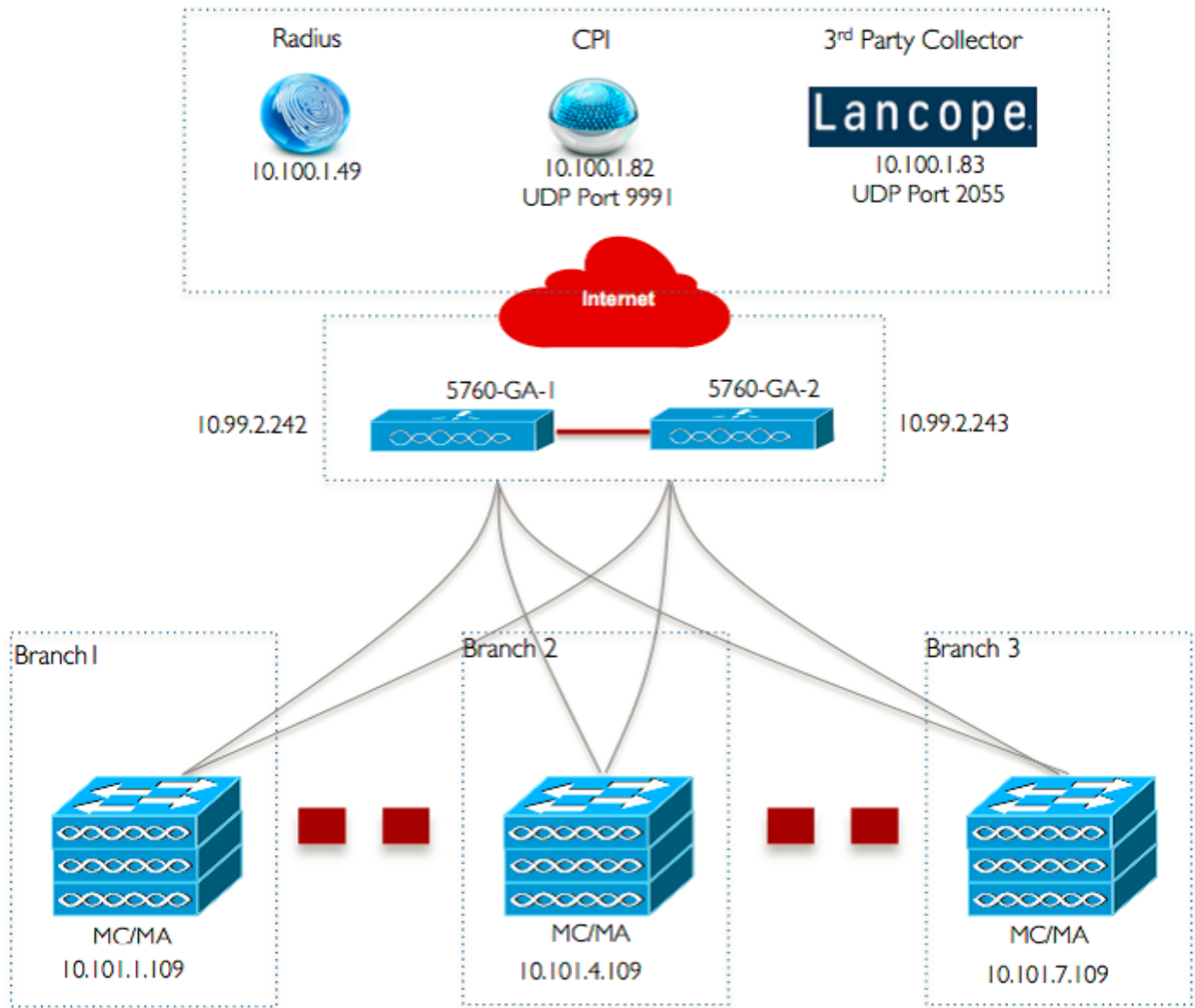
La sucursal remota o la empresa minorista tamaño pequeño puede consistir en un solo o un stack de los switches de Ethernet para proporcionar la conectividad de red a la haber atado con alambre y a los usuarios de red inalámbrica. Tales pequeñas redes pueden converger el Ethernet Switching con la capacidad inalámbrica de la última generación en el mismo switch de Catalyst.

Para tales diseños de red, el Switch puede integrar las funciones del regulador de la movilidad del regulador del Wireless LAN (WLC) y del agente de la movilidad (MA) sin requerir ningunos elementos convergidos adicionales del acceso, tales como Switch-Par-grupo (SPG) en la red. Estas redes pueden requerir los Servicios inalámbricos del invitado, así como la aplicación de la seguridad común y de la directiva de acceso a la red a través de todas las sucursales.

Configurar

Diagrama de la red

Esta imagen ilustra una topología de la referencia para una red derivada típica.



Configuraciones

Configuración de la capa baja 2/3

- **Modo del VLAN Trunk Protocol (VTP): Transparente**

Este ejemplo muestra la configuración del modo VTP.

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

- **Spanning Tree: Rápido-por el árbol de expansión de VLAN (PVST)**

Este ejemplo muestra la configuración Rápido-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 nombró a VLANs**

Este ejemplo muestra cómo se crean los VLA N.

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

- **Default gateway de la configuración**

La configuración del gateway predeterminado se muestra en este ejemplo.

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

- **Ruteo virtual y expedición (VRF) de la Administración de la configuración**

La configuración de VRF de la Administración se muestra en este ejemplo.

```
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
```

- **Snooping de la configuración IP DHCP**

En este ejemplo, el snooping del DHCP se configura para todos los VLA N del cliente de red inalámbrica.

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

Nota: Los puertos de link ascendente se deben marcar como confianza tal y como se muestra en del ejemplo de los puertos de link ascendente/del canal del puerto.

- **Examen del Address Resolution Protocol (ARP) de la configuración**

En este ejemplo, la inspección ARP se configura para todos los VLA N del cliente de red inalámbrica.

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

Nota: Los puertos de link ascendente se deben marcar como confianza tal y como se muestra en del ejemplo de los puertos de link ascendente/del canal del puerto.

- **Puertos de link ascendente/canal del puerto (permite los VLA N necesarios)**

En este ejemplo, se configura el puerto de link ascendente/el canal del puerto.

```
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
```

Movilidad

- **Interfaz de administración inalámbrica**

En este ejemplo, se habilitan las funciones inalámbricas y los 5760 WLC del ancla del invitado se configuran como el par de la movilidad.

```
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
```

Nota: Usted puede utilizar un WLC o 8510 AireOS de Cisco 5508 como regulador del ancla del invitado.

Seguridad

- **Parámetros globales**

Este ejemplo muestra la configuración de los Parámetros globales.

```
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
```

red inalámbrica (WLAN)

- **red inalámbrica (WLAN) del 802.1x**

La configuración de la red inalámbrica (WLAN) del 802.1x se muestra en este ejemplo.

```
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
```

- **red inalámbrica (WLAN) de la clave previamente compartida**

La configuración de la red inalámbrica (WLAN) de la clave previamente compartida se muestra en este ejemplo.

```
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
```

- **Abra la red inalámbrica (WLAN)**

La configuración abierta de la red inalámbrica (WLAN) se muestra en este ejemplo.

```
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 wpa no 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
```

Solución del invitado

- **red inalámbrica (WLAN) del invitado CWA**

La configuración de la red inalámbrica (WLAN) del invitado CWA se muestra en este ejemplo.

```
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
```

- **Configuración de la red inalámbrica (WLAN) de la movilidad y del invitado en el ancla 1 de**

5760 invitados

En este ejemplo, la red inalámbrica (WLAN) de la movilidad y del invitado se configura en el ancla 1. de 5760 invitados.

```
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
```

- **Reoriente el ACL para CWA (el Red-auth central)**

La configuración para reorientar el ACL para CWA se muestra en este ejemplo.

```
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
```

Servicios inalámbricos avanzados IOS

- **Visibilidad de la aplicación y configuración del control (AVC)**

Este ejemplo muestra la configuración de 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
```

- **Configuración de la red inalámbrica (WLAN)**

Este ejemplo muestra la configuración de la red inalámbrica (WLAN).

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


- **Shaping del ancho de banda de egreso para los WLAN**

El ejemplo muestra la configuración del shaping del ancho de banda de egreso para los 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
```

- **Configuración de la red inalámbrica (WLAN)**

Este ejemplo muestra la configuración de la red inalámbrica (WLAN).

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

Mejores medidas

Las mejores prácticas para la configuración de red inalámbrica incluyen:

- Usando el comando del rápido-SSID-cambio del cliente de red inalámbrica de configurar el cambio rápido SSID.
- Usando el cifrado del passwd encendido y la clave del passwd ofusque los comandos para la encriptación de contraseña.