Configuración del acceso convergente en una red de sucursal pequeña con un solo switch

Contenido

Introducción

Este documento proporciona configuraciones de ejemplo para la implementación de acceso convergente en una red de switch único de una sucursal pequeña. Estas configuraciones se pueden utilizar en cientos o incluso miles de sucursales para implementar la red inalámbrica en las sucursales con configuraciones probadas.

Prerequisites

Requirements

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
- Cisco IOS versión 03.03.00SE o posterior
- Cisco IES versión 1.2 o posterior

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.

Antecedentes

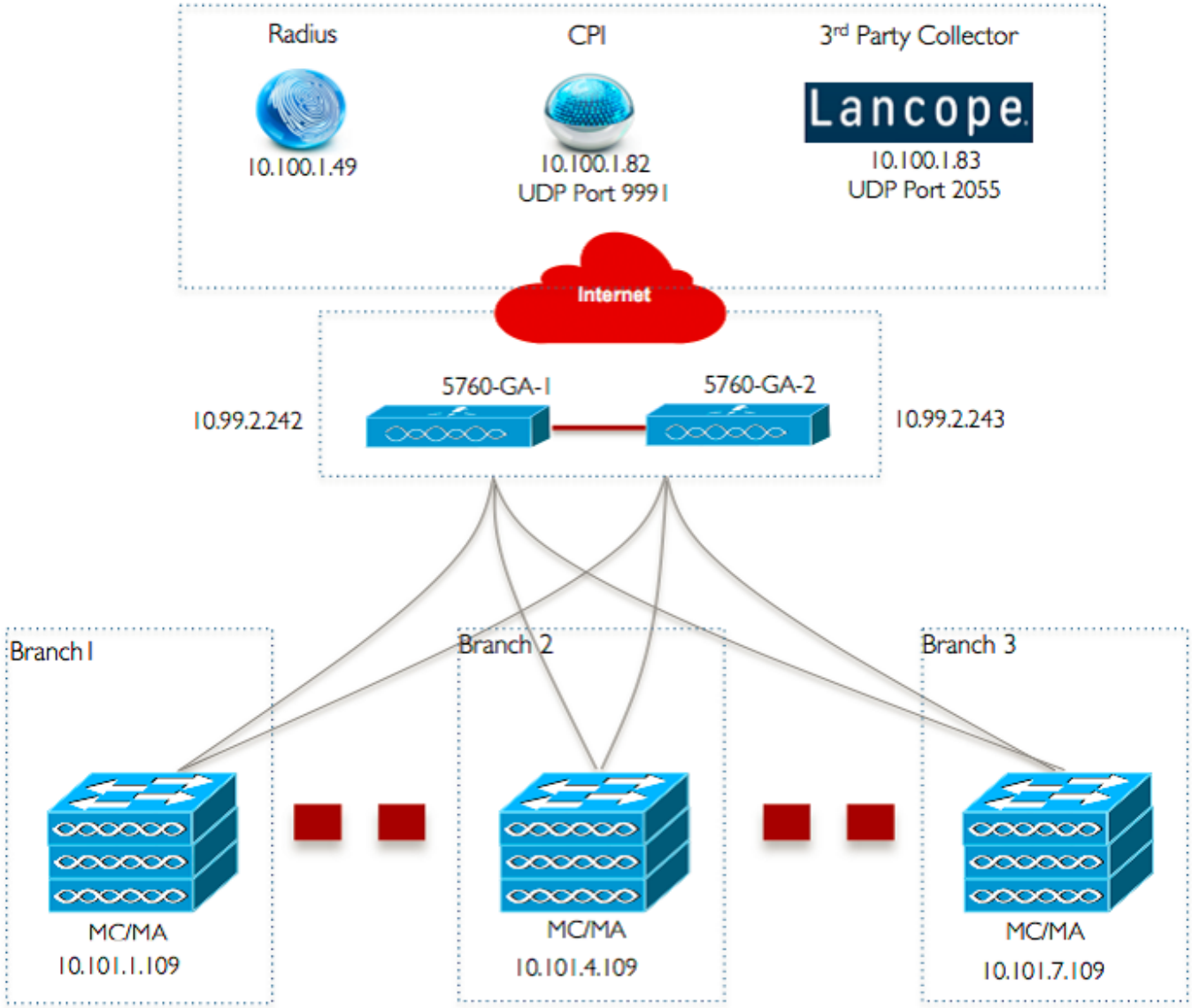
La pequeña sucursal remota o tienda minorista puede constar de una o varias pilas de switches Ethernet para proporcionar conectividad de red a los usuarios con cables e inalámbricos. Estas redes pequeñas pueden hacer converger el switching Ethernet con la capacidad inalámbrica de última generación en el mismo switch Catalyst.

Para estos diseños de red, el switch puede integrar las funciones del controlador de movilidad del controlador de LAN inalámbrica (WLC) y del agente de movilidad (MA) sin necesidad de ningún elemento de acceso convergente adicional, como el grupo de peers del switch (SPG) en la red. Estas redes pueden requerir servicios inalámbricos para invitados, así como la aplicación de políticas de acceso a la red y seguridad comunes en todas las sucursales.

Configurar

Diagrama de la red

Esta imagen ilustra una topología de referencia para una red de sucursal típica.



Configuraciones

Configuración de capa 2/3 básica

- **Modo de protocolo troncal VLAN (VTP): Transparente**

Este ejemplo muestra la configuración del modo VTP.

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

- **Spanning Tree: Árbol de expansión rápido por VLAN (PVST)**

Este ejemplo muestra la configuración 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
```

- Crear VLAN con nombre

Este ejemplo muestra cómo se crean las VLAN.

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

- Configurar gateway predeterminado

En este ejemplo se muestra la configuración de la puerta de enlace predeterminada.

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

- Configuración del routing y reenvío virtuales (VRF) de gestión

En este ejemplo se muestra la configuración de VRF de administración.

```
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
```

- Configuración de IP DHCP Snooping

En este ejemplo, la indagación DHCP se configura para todas las VLAN de cliente inalámbricas.

```
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 enlace ascendente deben marcarse como de confianza, como se muestra en el ejemplo Puertos de enlace ascendente/Canal de puerto.

- Inspección del protocolo de resolución de direcciones (ARP)

En este ejemplo, la inspección ARP se configura para todas las VLAN de cliente inalámbricas.

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

> **Nota:** Los puertos de enlace ascendente deben marcarse como de confianza, como se muestra en el ejemplo Puertos de enlace ascendente/Canal de puerto.

- **Puertos de enlace ascendente/Canal de puerto (permitir las VLAN necesarias)**

En este ejemplo, se configura Uplink Port/Port-Channel.

```
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 gestión inalámbrica**

En este ejemplo, se habilita la funcionalidad inalámbrica y el WLC 5760 Guest Anchor se configura como el peer de 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: Puede utilizar un WLC Cisco 5508 o un AireOS 8510 como controlador de anclaje invitado.

Security

- **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
```

WLAN

- **WLAN 802.1X**

En este ejemplo se muestra la configuración de WLAN 802.1X.

```
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 de clave precompartida

En este ejemplo se muestra la configuración de WLAN de clave precompartida.

```
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
```

- WLAN abierta

En este ejemplo se muestra la configuración de WLAN abierta.

```
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
```

Solución para invitados

- WLAN de invitado CWA

En este ejemplo se muestra la configuración de WLAN de invitado de CWA.

```
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 movilidad y WLAN de invitado en 5760 Guest Anchor 1

En este ejemplo, la WLAN de invitado y movilidad se configura en el anclaje de invitado 5760 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
```

- Redirección de ACL para CWA (autenticación web central)

En este ejemplo se muestra la configuración para redirigir ACL para CWA.

```
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 IOS avanzados

- Configuración de Visibilidad y control de aplicaciones (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 WLAN**

Este ejemplo muestra la configuración de WLAN.

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

- **Modelado de ancho de banda de egreso para WLAN**

El ejemplo muestra la configuración del modelado de ancho de banda de salida para las 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 WLAN**

Este ejemplo muestra la configuración de WLAN.

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

Mejores medidas

Entre las prácticas recomendadas para la configuración inalámbrica se incluyen las siguientes:

- Uso del comando **wireless client fast-ssid-change** para configurar el rápido cambio de SSID.
- El uso de los comandos **passwd encryption on** y **passwd key obfuscate** para el cifrado de contraseñas.