

# Configurar o acesso convergido em uma rede de filial pequena do switch único

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Mobilidade](#)

[Segurança](#)

[WLAN](#)

[Solução do convidado](#)

[Serviços sem fio avançados IO](#)

[Melhores práticas](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento fornece configurações de amostra para o desenvolvimento convergido do acesso em uma rede do switch único do pequeno-ramo. Estas configurações podem ser usadas através das centenas ou mesmo dos milhares de ramos para distribuir a rede Wireless nas localidades da ruptura com - e - as configurações testadas experimentadas.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 3850 Series Switch
- Versão do Cisco IOS 03.03.00SE ou mais tarde
- Versão 1.2 ou mais recente do LES de Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

## **Informações de Apoio**

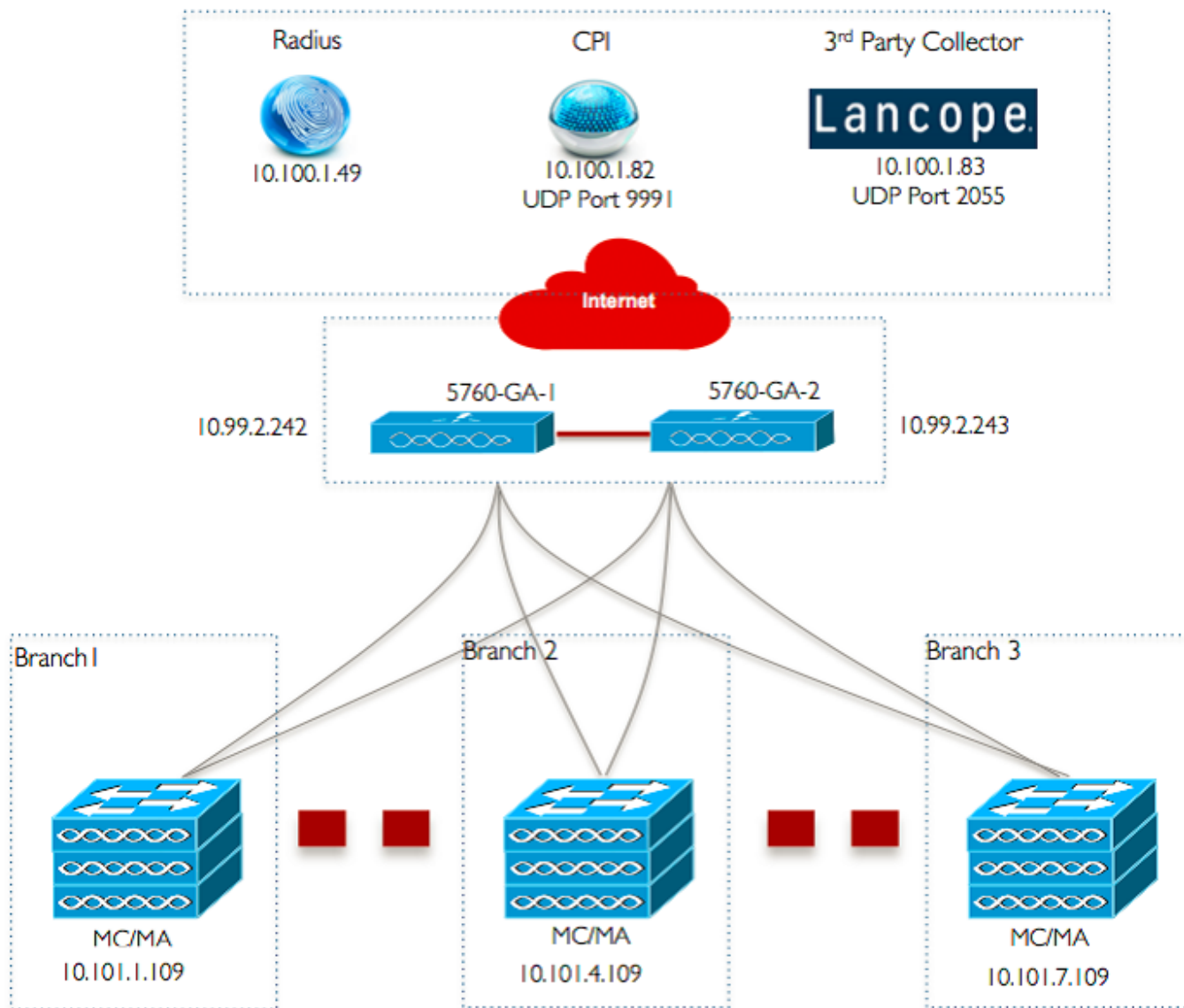
O escritório remoto ou a loja de varejo do pequeno-tamanho podem consistir em um único ou em uma pilha de Switch Ethernet para fornecer a conectividade de rede ao prendido e aos usuários Wireless. Tais redes pequenas podem convergir o switching de Ethernet com capacidade wireless da próxima geração no mesmo Catalyst Switch.

Para tais projetos de rede, o interruptor pode integrar funções do controlador da mobilidade do controlador do Wireless LAN (WLC) e do agente da mobilidade (MA) sem exigir nenhuns elementos convergidos adicionais do acesso, tais como o Interruptor-Par-grupo (SPG) na rede. Estas redes podem exigir Serviços sem fio do convidado, assim como reforço de política da segurança comum e do acesso de rede através de todos os escritórios filiais.

## **Configurar**

### **Diagrama de Rede**

Esta imagem ilustra uma topologia da referência para uma rede de filial típica.



## Configurações

### Configuração da camada baixa 2/3

- **Modo do protocolo VLAN Trunk (VTP): Transparente**

Este exemplo mostra a configuração do modo de VTP.

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

- **Medida - árvore: Rápido-pelo Spanning Tree de VLAN (PVST)**

Este exemplo mostra a configuração 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 nomeou VLAN**

Este exemplo mostra como os VLAN são criados.

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

- **Configurar o gateway padrão**

A configuração de gateway de voz padrão é mostrada neste exemplo.

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

- **Configurar o roteamento virtual do Gerenciamento e a transmissão (o VRF)**

A configuração de VRF do Gerenciamento é mostrada neste exemplo.

```
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
```

- **Configurar a espiação IP DHCP**

Neste exemplo, a espiação DHCP é configurada para todo o cliente Wireless 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
```

Nota: As portas de uplink devem ser marcadas como a confiança segundo as indicações do exemplo das portas de uplink/canal de porta.

- **Configurar a inspeção do Address Resolution Protocol (ARP)**

Neste exemplo, a inspeção ARP é configurada para todo o cliente Wireless VLAN.

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

Nota: As portas de uplink devem ser marcadas como a confiança segundo as indicações do exemplo das portas de uplink/canal de porta.

- **Portas de uplink/canal de porta (permita VLAN necessários)**

Neste exemplo, a porta de uplink/canal de porta é configurada.

```
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
```

## Mobilidade

- **Interface de gerenciamento wireless**

Neste exemplo, a funcionalidade wireless é permitida e a âncora WLC de 5760 convidados é configurada como o par da mobilidade.

```
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: Você pode usar Cisco 5508 WLC ou uns 8510 AireOS como um controlador da âncora do convidado.

## Segurança

- **Parâmetros globais**

Este exemplo mostra a configuração dos parâmetros globais.

```
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**

A configuração do 802.1X WLAN é mostrada neste exemplo.

```
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
```

- **Chave pré-compartilhada WLAN**

A configuração da chave pré-compartilhada WLAN é mostrada neste exemplo.

```
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 o WLAN**

A configuração aberta WLAN é mostrada neste exemplo.

```
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
```

## Solução do convidado

- **Convidado WLAN CWA**

A configuração do convidado WLAN CWA é mostrada neste exemplo.

```
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
```

- **Configuração da mobilidade e do convidado WLAN na âncora 1 de 5760 convidados**

Neste exemplo, a mobilidade e o convidado WLAN são configurados na âncora 1. de 5760 convidados.

```
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 o ACL para CWA (o Web-AUTH central)**

A configuração para reorientar o ACL para CWA é mostrada neste exemplo.

```
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
```

## Serviços sem fio avançados IO

- **Configuração da visibilidade e do controle do aplicativo (AVC)**

Este exemplo mostra a configuração 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
```

- **Configuração WLAN**

Este exemplo mostra a configuração do WLAN.

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

- **Largura de banda de saída que dá forma para WLAN**

O exemplo mostra a configuração da largura de banda de saída que dá forma para WLAN.

```
policy-map ABCCorp-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
```

## • Configuração WLAN

Este exemplo mostra a configuração do WLAN.

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

## Melhores práticas

Os melhores prática para a configuração sem fio incluem:

- Usando a **rápido-SSID-mudança do cliente Wireless** comande para configurar a mudança rápida SSID.
- Usando a **criptografia da senha sobre** e a **chave da senha confunda** comandos para a criptografia de senha.