Configurar o acesso convergido em uma rede de filial pequena com um único switch

Contents

Introdução

Este documento fornece configurações de exemplo para a implantação do Acesso Convergido em uma rede de switch simples de filial pequena. Essas configurações podem ser usadas em centenas ou até milhares de filiais para implantar a rede sem fio nas filiais com configurações testadas e comprovadas.

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
- Cisco IOS versão 03.03.00SE ou posterior
- Cisco IES versão 1.2 ou posterior

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

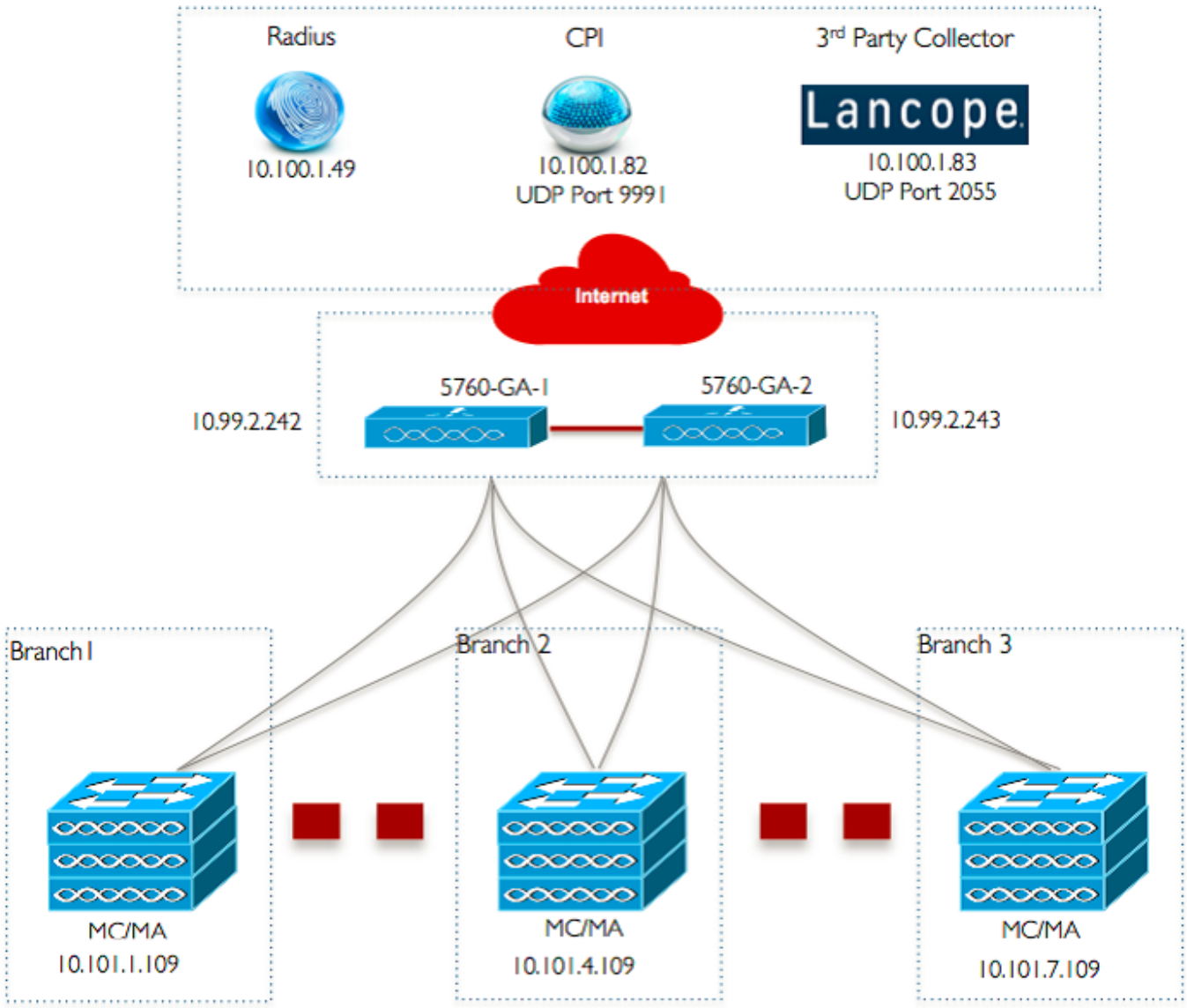
A filial ou loja de varejo remota de pequeno porte pode consistir em um único switch Ethernet ou em uma pilha de switches Ethernet para fornecer conectividade de rede aos usuários com e sem fio. Essas redes pequenas podem convergir o switching de Ethernet com o recurso sem fio de próxima geração no mesmo switch do Catalyst.

Para esses projetos de rede, o switch pode integrar as funções do controlador de mobilidade da controladora Wireless LAN (WLC) e do agente de mobilidade (MA) sem exigir nenhum elemento adicional de acesso convergido, como o Switch-Peer-Group (SPG) na rede. Essas redes podem exigir serviços sem fio para convidados, bem como a aplicação de políticas comuns de segurança e acesso à rede em todas as filiais.

Configurar

Diagrama de Rede

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



Configurações

Configuração básica de camada 2/3

- Modo do VLAN Trunk Protocol (VTP): Transparente

Este exemplo mostra a configuração do modo VTP.

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

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

Este exemplo mostra a configuração do 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
```

- Criar VLANs nomeadas

Este exemplo mostra como as VLANs são criadas.

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

- Configurar gateway padrão

A configuração do gateway 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 e Encaminhamento Virtual (VRF) de Gerenciamento

A configuração do VRF de 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 rastreamento de DHCP IP

Neste exemplo, o rastreamento de DHCP é configurado para todas as VLANs de clientes sem fio.

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

Observação: as portas de uplink devem ser marcadas como confiáveis, conforme mostrado no exemplo Portas de Uplink/Canal de Porta.

- Configurar a inspeção do Address Resolution Protocol (ARP)

Neste exemplo, a inspeção ARP é configurada para todas as VLANs de clientes sem fio.

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

Observação: as portas de uplink devem ser marcadas como confiáveis, conforme mostrado no exemplo Portas de Uplink/Canal de Porta.

- Portas de uplink/canal de porta (permitir as VLANs necessárias)

Neste exemplo, o Uplink Port/Port-Channel está configurado.

```
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 sem fio

Neste exemplo, a funcionalidade sem fio é habilitada e a WLC 5760 Guest Anchor é configurada como o peer de 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 um Cisco 5508 WLC ou um 8510 AireOS como um controlador âncora convidado.

Security

- Parâmetros Globais

Este exemplo mostra a configuração de 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

- WLAN 802.1X

A configuração da WLAN 802.1X 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
```

- WLAN de chave pré-compartilhada

A configuração da WLAN da chave pré-compartilhada 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
```

- Abrir WLAN

A configuração Open 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 para convidados

- WLAN de convidado do CWA

A configuração da WLAN de convidado do 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
```

- Mobilidade e configuração de Guest WLAN no 5760 Guest Anchor 1

Neste exemplo, a Mobilidade e a Guest WLAN são configuradas no 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
```

- Redirecionar ACL para CWA (Web-Auth central)

A configuração para redirecionar 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 IOS avançados

- Configuração do Application Visibility and Control (AVC)

Este exemplo mostra a configuração do 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 de WLAN

Este exemplo mostra a configuração da WLAN.

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

- Modelagem de largura de banda de saída para WLANs

O exemplo mostra a configuração da modelagem da largura de banda de saída para WLANs.

```
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
```

- Configuração de WLAN

Este exemplo mostra a configuração da WLAN.

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

Melhores práticas

As práticas recomendadas para a configuração sem fio incluem:

- Usando o comando wireless client fast-ssid-change para configurar a alteração rápida de SSID.
- Usando os comandos passwd encryption on e passwd key obfuscate para criptografia de senha.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.