Geconversierde toegang configureren in een netwerk met één switch voor kleine takken

Inhoud

Inleiding

Dit document biedt voorbeeldconfiguraties voor geconvergeerde toegangsinstallatie in een netwerk met één schakelaar voor kleine takken. Deze configuraties kunnen over honderden of zelfs duizenden takken worden gebruikt om het draadloze netwerk op de takplaatsen met beproefde en geteste configuraties in te zetten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 3850 Series switch
- Cisco IOS versie 3.03.00SE of hoger
- Cisco IOS versie 1.2 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van

elke opdracht begrijpen.

Achtergrondinformatie

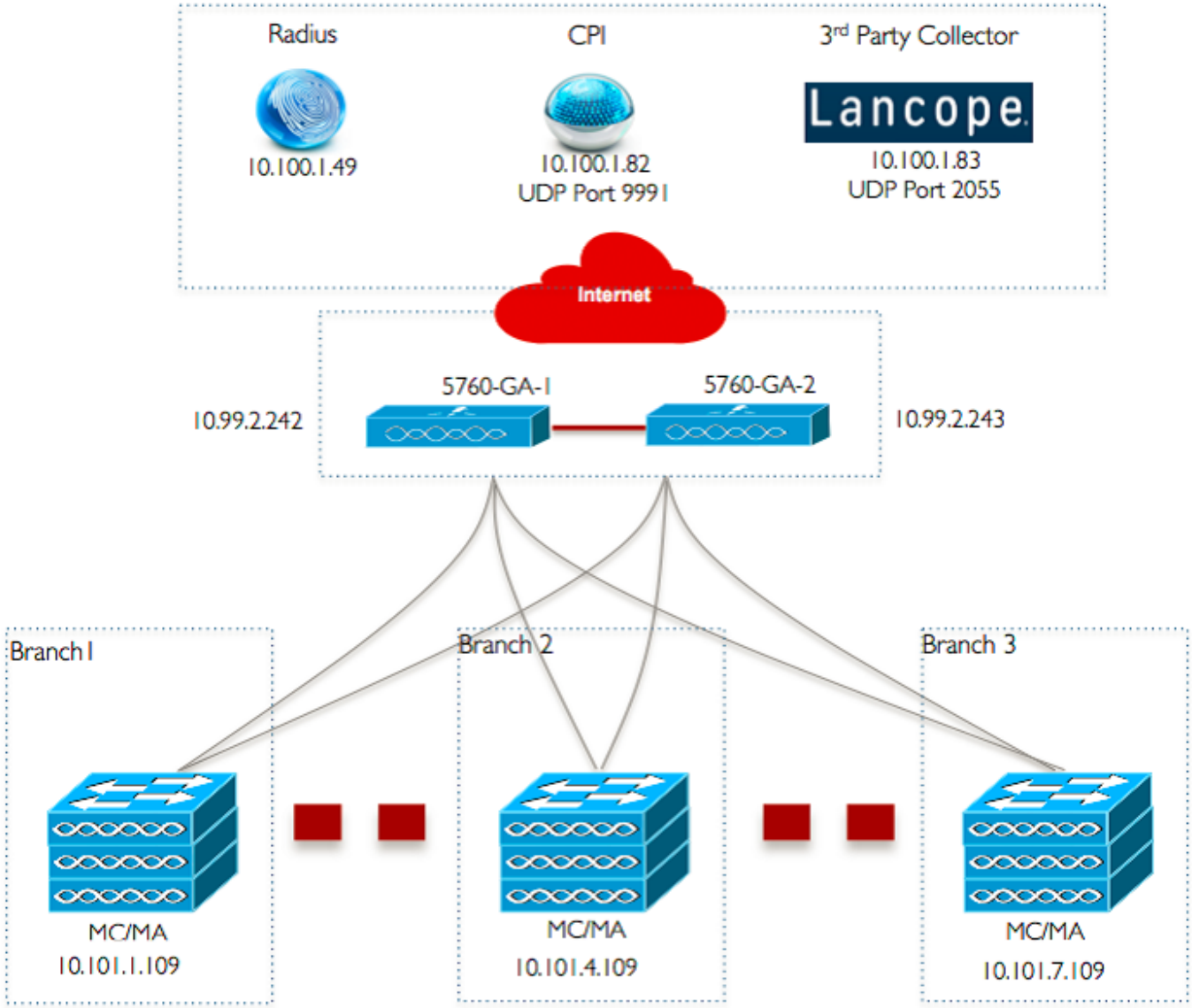
De kleine verafgelegen filiaal of detailhandel kan uit één enkele of een stapel Ethernet switches bestaan om netwerkconnectiviteit aan de bekabelde en draadloze gebruikers te bieden. Zulke kleine netwerken kunnen de Ethernet-switching converteren met de volgende generatie draadloze mogelijkheden op dezelfde katalysator.

Voor dergelijke netwerkontwerpen kan de schakelaar de functies van de Draadloze LAN Controller (WLC) mobiliteitscontroller en de mobiliteitsagent (MA) integreren zonder extra geconvergeerde access elementen, zoals Switch-peer-Group (SPG) in het netwerk te vereisen. Deze netwerken kunnen de mobiele diensten van de gast vereisen, evenals de gemeenschappelijke handhaving van het veiligheids- en netwerktoegangsbeleid over alle bijkantoren.

Configureren

Netwerkdiagram

Dit beeld illustreert een referentietechnologie voor een typisch aftakknetwerk.



Configuraties

Base Layer 2/3 configuratie

- **VLAN Trunk Protocol (VTP)-modus: Doorzichtig**

Dit voorbeeld toont de configuratie van VTP-modus.

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

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

Dit voorbeeld toont de snelle-PVST configuratie.

```
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree portfast bpdufilter default
spanning-tree extend system-id
```

- **Geselecteerde VLAN's maken**

Dit voorbeeld laat zien hoe de VLAN's worden gemaakt.

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

- **Standaardgateway instellen**

De configuratie van de standaardgateway wordt in dit voorbeeld getoond.

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

- **Beheer virtuele routing en doorsturen (VRF) configureren**

De configuratie van het Beheer VRF wordt in dit voorbeeld getoond.

```
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
```

- **IP DHCP-signalering configureren**

In dit voorbeeld wordt DHCP-snooping ingesteld voor alle draadloze client-VLAN's.

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

> Opmerking: Uplink-poorten moeten worden gemarkeerd als vertrouwen, zoals in het voorbeeld Uplink-poorten/Port-Channel wordt getoond.

- **Configuratie van Protocol voor adresoplossing (ARP)-inspectie**

In dit voorbeeld wordt de ARP-inspectie ingesteld voor alle draadloze client-VLAN's.

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

> Opmerking: Uplink-poorten moeten worden gemarkeerd als vertrouwen, zoals in het voorbeeld Uplink-poorten/Port-Channel wordt getoond.

- **Uplink-poorten/Port-Channel (enabled-VLAN's)**

In dit voorbeeld wordt de uplinks Port/Port-Channel geconfigureerd.

```
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
```

Mobiliteit

- **Draadloze beheerinterface**

In dit voorbeeld wordt draadloze functionaliteit ingeschakeld en wordt de 5760 Guest Anchor WLC ingesteld als een mobiliteitspeer.

```
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
```

> **Opmerking**: u kunt een Cisco 5508 WLC of een 8510 AireOS gebruiken als een gastpresentator-controller.

Security

- **Mondiale parameters**

Dit voorbeeld toont de configuratie van mondiale parameters.

```
       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**

De 802.1X WLAN-configuratie wordt in dit voorbeeld weergegeven.

```
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
```

- Vooraf gedeelde sleutel WLAN

De pre-Shared Key WLAN-configuratie wordt in dit voorbeeld getoond.

```
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
```

- Open WLAN

De configuratie van Open WLAN-software wordt in dit voorbeeld weergegeven.

```
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
```

Guest Solution

- CWA Guest WLAN

De CWA Guest WLAN-configuratie wordt in dit voorbeeld weergegeven.

```
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
```

- Mobility en Guest WLAN-configuratie op 5760 Guest Anchor 1

In dit voorbeeld worden Mobility en Guest WLAN geconfigureerd op 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
```

- Omleiden ACL voor CWA (Centraal Web-Auth)

In dit voorbeeld wordt de configuratie om ACL voor CWA om te buigen weergegeven.

```
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
```

Geavanceerde IOS draadloze services

- Configuratie van Application Visibility and Control (AVC)

Dit voorbeeld toont de configuratie van 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
```

- **WLAN-configuratie**

Dit voorbeeld toont de configuratie van WLAN.

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

- **Grijsbandbreedte-shaping voor WLAN's**

Het voorbeeld toont de configuratie van uitgaande Bandbreedte-vormgeving voor WLAN's.

```
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
```

- **WLAN-configuratie**

Dit voorbeeld toont de configuratie van WLAN.

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

Beste praktijken

Best practices voor draadloze configuratie zijn:

- Gebruik van het **draadloze client fast-change** opdracht om snel SSID te configureren.
- Gebruik van de **brede encryptie op de** opdrachten voor het verduisteren van de wachtwoorden **en** het **passwd**.