Konfiguration von konvergentem Zugriff in einem kleinen Zweigstellennetzwerk mit einem Switch

Inhalt

Einführung

Dieses Dokument enthält Beispielkonfigurationen für die Bereitstellung von konvergentem Zugriff in einem kleinen Zweigstellennetzwerk mit einem Switch. Diese Konfigurationen können in Hunderten oder sogar Tausenden von Zweigstellen verwendet werden, um das Wireless-Netzwerk in den Zweigstellen mit bewährten Konfigurationen bereitzustellen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switch der Serie 3850
- Cisco IOS Version 03.03.00SE oder höher
- Cisco IES ab Version 1.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

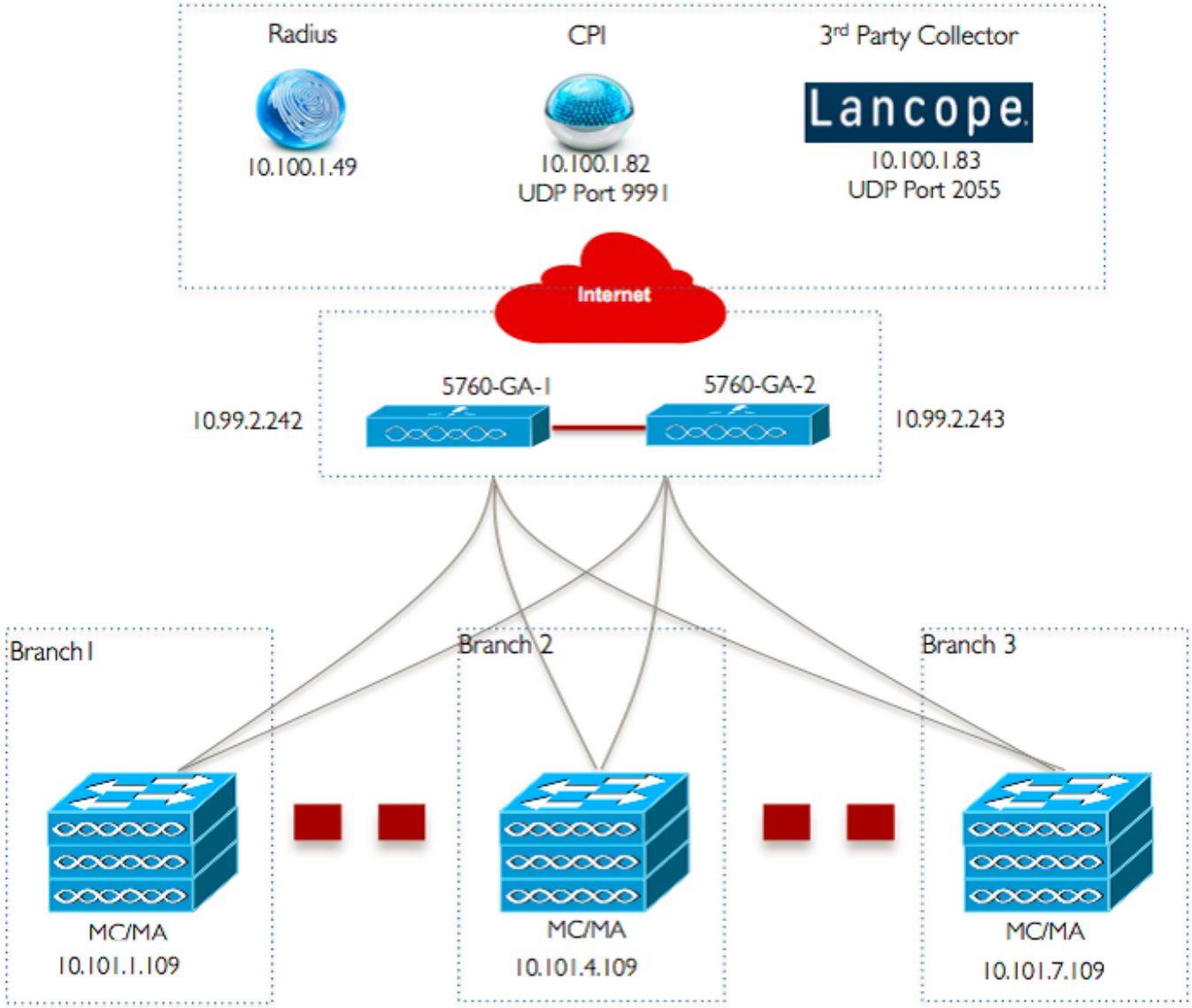
Die kleine Zweigstelle oder der kleine Einzelhandelsgeschäft kann aus einem einzelnen oder einem Stack von Ethernet-Switches bestehen, um kabelgebundenen und Wireless-Benutzern Netzwerkverbindungen bereitzustellen. Solche kleinen Netzwerke können Ethernet-Switching mit Wireless-Funktionen der nächsten Generation auf demselben Catalyst-Switch konvergieren.

Bei solchen Netzwerkdesigns kann der Switch Wireless LAN Controller (WLC) Mobility Controller- und Mobility Agent (MA)-Funktionen integrieren, ohne dass zusätzliche Converged Access-Elemente wie die Switch-Peer-Gruppe (SPG) im Netzwerk erforderlich sind. Diese Netzwerke können Wireless-Services für Gäste sowie eine einheitliche Durchsetzung von Sicherheits- und Netzwerkzugriffsrichtlinien in allen Zweigstellen erfordern.

Konfigurieren

Netzwerkdiagramm

Dieses Bild zeigt eine Referenztopologie für ein typisches Zweigstellennetzwerk.



Konfigurationen

Basis-Layer-2/3-Konfiguration

- **VTP-Modus (VLAN Trunk Protocol): Transparent**

Dieses Beispiel zeigt die Konfiguration des VTP-Modus.

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

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

Dieses Beispiel zeigt die Rapid-PVST-Konfiguration.

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

- **Benannte VLANs erstellen**

Dieses Beispiel zeigt, wie die VLANs erstellt werden.

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

- **Standard-Gateway konfigurieren**

Die Konfiguration des Standard-Gateways ist in diesem Beispiel dargestellt.

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

- **Konfigurieren von Management Virtual Routing and Forwarding (VRF)**

Die Management-VRF-Konfiguration ist in diesem Beispiel dargestellt.

```
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
```

- **Konfigurieren von IP-DHCP-Snooping**

In diesem Beispiel wird DHCP-Snooping für alle Wireless-Client-VLANs konfiguriert.

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

> **Hinweis**: Uplink-Ports müssen als vertrauenswürdig markiert sein, wie im Beispiel für Uplink-Ports/Port-Channel gezeigt.

- **Konfigurieren der ARP-Inspektion (Address Resolution Protocol)**

In diesem Beispiel wird die ARP-Inspektion für alle Wireless-Client-VLANs konfiguriert.

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

> **Hinweis**: Uplink-Ports müssen als vertrauenswürdig markiert sein, wie im Beispiel für Uplink-Ports/Port-Channel gezeigt.

- **Uplink-Ports/Port-Channel (für erforderliche VLANs)**

In diesem Beispiel wird Uplink-Port/Port-Channel konfiguriert.

```
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
```

Mobilität

- **Wireless-Management-Schnittstelle**

In diesem Beispiel ist die Wireless-Funktion aktiviert, und der WLC 5760 Guest Anchor wird als Mobility Peer konfiguriert.

```
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
```

Hinweis:Sie können einen Cisco 5508 WLC oder einen 8510 AireOS als Gastanker-Controller verwenden.

Sicherheit

- **Globale Parameter**

In diesem Beispiel wird die Konfiguration globaler Parameter veranschaulicht.

```
       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**

In diesem Beispiel wird die 802.1X-WLAN-Konfiguration gezeigt.

```
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 mit vorinstalliertem Schlüssel

Die WLAN-Konfiguration für den Pre-Shared Key ist in diesem Beispiel dargestellt.

```
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
```

- Offenes WLAN

In diesem Beispiel wird die Open WLAN-Konfiguration gezeigt.

```
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
```

Gastlösung

- CWA Gast-WLAN

In diesem Beispiel wird die CWA-Gast-WLAN-Konfiguration gezeigt.

```
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
```

- WLAN-Konfiguration für Mobilität und Gäste auf 5760 Guest Anchor 1

In diesem Beispiel wird Mobility and Guest WLAN auf 5760 Guest Anchor 1 konfiguriert.

```
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
```

- ACL umleiten für CWA (zentrale Web-Auth)

Die Konfiguration zur Umleitung der ACL für CWA ist in diesem Beispiel dargestellt.

```
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
```

Erweiterte IOS Wireless-Services

- AVC-Konfiguration (Application Visibility and Control)

Dieses Beispiel zeigt die Konfiguration von 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-Konfiguration**

Dieses Beispiel zeigt die Konfiguration von WLAN.

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

- **Egress Bandwidth Shaping für WLANs**

Das Beispiel zeigt die Konfiguration von Egress Bandwidth Shaping für 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
```

- **WLAN-Konfiguration**

Dieses Beispiel zeigt die Konfiguration von WLAN.

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

Best Practices

Zu den Best Practices für die Wireless-Konfiguration gehören:

- Verwenden des Befehls **Schneller** SSID**-Wechsel** für den **Wireless-Client**, um schnelle Änderungen der SSID zu konfigurieren.
- Die Verwendung der **Passwort-Verschlüsselung auf** und des **Passwort-Schlüssels** für die Passwortverschlüsselung.