단일 스위치 소규모 지사 네트워크에서 통합 액세스 구성

목차

소개

이 문서에서는 소규모 브랜치 단일 스위치 네트워크에서 컨버지드 액세스 구축을 위한 샘플 컨피그레이션을 제공합니다.이러한 컨피그레이션은 수백 또는 수천 개의 브랜치에서 테스트되고 테스트된 컨피그레이션으로 지사에 무선 네트워크를 구축하는 데 사용할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 3850 Series 스위치
- Cisco IOS 버전 03.03.00SE 이상
- Cisco ISE 버전 1.2 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

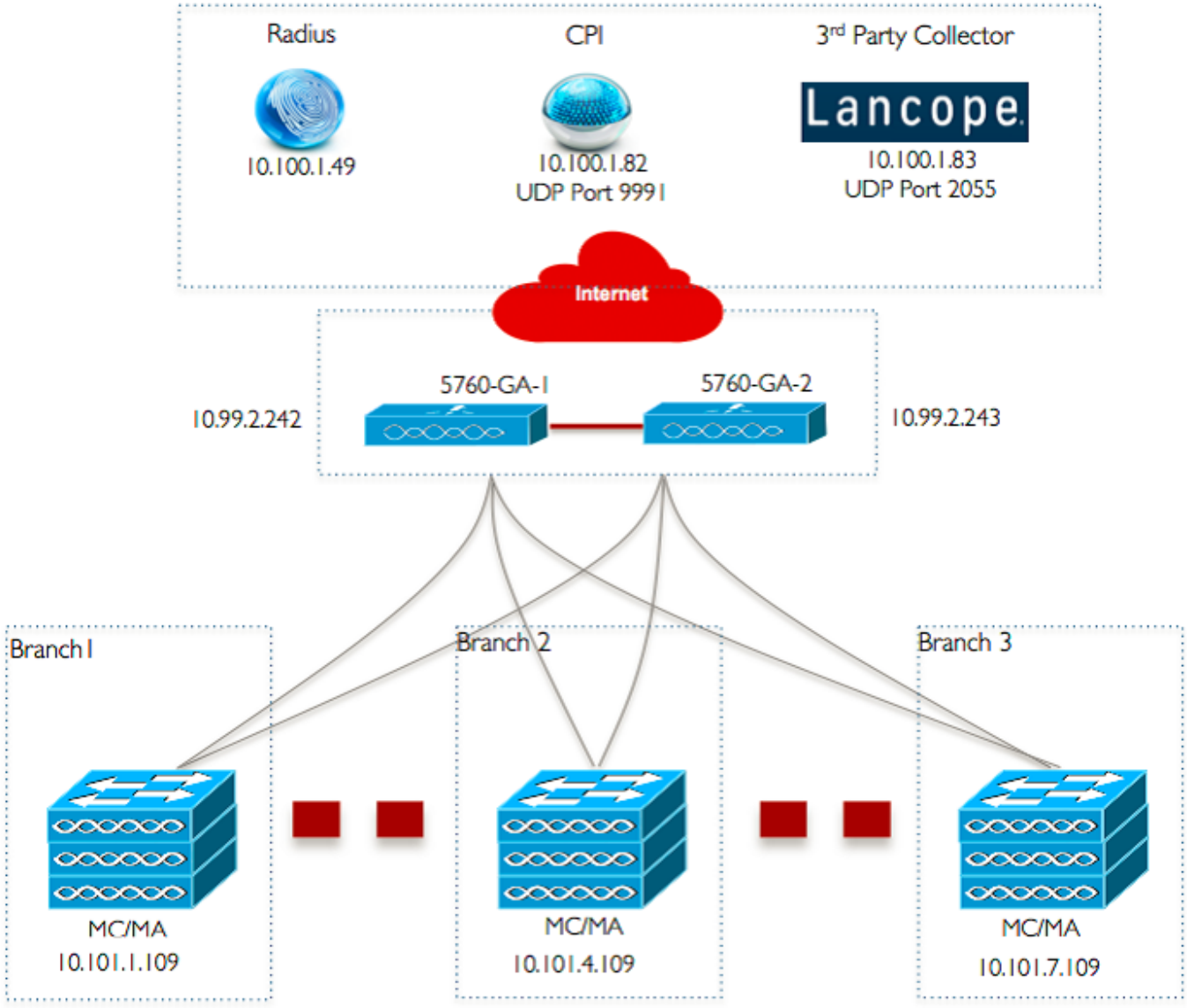
소규모 원격 지사 또는 소매점은 단일 또는 하나의 이더넷 스위치 스택으로 구성될 수 있어 유선 및 무선 사용자에게 네트워크 연결을 제공할 수 있습니다.이러한 소규모 네트워크는 동일한 Catalyst 스위치에서 이더넷 스위칭을 차세대 무선 기능으로 통합할 수 있습니다.

이러한 네트워크 설계의 경우 스위치는 네트워크에 SPG(Switch-Peer-Group)와 같은 추가 통합 액세스 요소가 필요 없이 WLC(Wireless LAN Controller) 모빌리티 컨트롤러 및 모빌리티 에이전트(MA) 기능을 통합할 수 있습니다.이러한 네트워크에는 게스트 무선 서비스는 물론 모든 지사에서 공통된 보안 및 네트워크 액세스 정책을 적용해야 할 수 있습니다.

구성

네트워크 다이어그램

이 이미지는 일반적인 브랜치 네트워크에 대한 참조 토폴로지를 보여줍니다.



구성

기본 레이어 2/3 컨피그레이션

- **VTP(VLAN Trunk Protocol) 모드:투명**

이 예에서는 VTP 모드의 컨피그레이션을 보여줍니다.

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

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

이 예에서는 Rapid-PVST 컨피그레이션을 보여줍니다.

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

- **명명된 VLAN 생성**

이 예에서는 VLAN이 생성되는 방법을 보여줍니다.

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

- **기본 게이트웨이 구성**

이 예에서는 기본 게이트웨이 컨피그레이션이 표시됩니다.

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

- **VRF(Management Virtual Routing and Forwarding) 구성**

이 예에서는 관리 VRF 컨피그레이션이 표시됩니다.

```
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 스누핑 구성**

이 예에서는 모든 무선 클라이언트 VLAN에 대해 DHCP 스누핑이 구성됩니다.

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

참고:업링크 포트는 업링크 포트/포트-채널 예에 표시된 것처럼 신뢰로 표시되어야 합니다.

- **ARP(Address Resolution Protocol) 검사 구성**

이 예에서는 모든 무선 클라이언트 VLAN에 대해 ARP 검사가 구성됩니다.

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

참고:업링크 포트는 업링크 포트/포트-채널 예에 표시된 것처럼 신뢰로 표시되어야 합니다.

- **업링크 포트/포트 채널(필요한 VLAN 허용)**

이 예에서는 업링크 포트/포트-채널이 구성됩니다.

```
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
```

모빌리티

- **무선 관리 인터페이스**

이 예에서는 무선 기능이 활성화되고 5760 Guest Anchor WLC가 모빌리티 피어로 구성됩니다.

```
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
```

참고:Cisco 5508 WLC 또는 8510 AireOS를 게스트 앵커 컨트롤러로 사용할 수 있습니다.

보안

- **전역 매개변수**

이 예에서는 전역 매개변수의 컨피그레이션을 보여줍니다.

```
       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**

이 예에는 802.1X WLAN 컨피그레이션이 나와 있습니다.

```
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
```

- **사전 공유 키 WLAN**

이 예에는 사전 공유 키 WLAN 컨피그레이션이 나와 있습니다.

```
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 열기**

이 예에서는 Open WLAN 컨피그레이션이 표시됩니다.

```
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
```

게스트 솔루션

- **CWA 게스트 WLAN**

이 예에서는 CWA 게스트 WLAN 컨피그레이션이 표시됩니다.

```
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
```

- **5760 게스트 앵커 1의 모빌리티 및 게스트 WLAN 구성**

이 예에서 모빌리티 및 게스트 WLAN은 5760 게스트 앵커 1에 구성됩니다.

```
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
```

- **CWA에 대한 리디렉션 ACL(중앙 웹 인증)**

이 예에는 CWA에 대한 ACL을 리디렉션하는 컨피그레이션이 나와 있습니다.

```
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
```

고급 IOS 무선 서비스

- **AVC(Application Visibility and Control) 컨피그레이션**

이 예에서는 AVC의 컨피그레이션을 보여줍니다.

```
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 컨피그레이션**

이 예에서는 WLAN의 컨피그레이션을 보여줍니다.

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

- **WLAN을 위한 이그레스 대역폭 셰이핑**

이 예에서는 WLAN에 대한 이그레스 대역폭 셰이핑의 컨피그레이션을 보여줍니다.

```
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 컨피그레이션**

이 예에서는 WLAN의 컨피그레이션을 보여줍니다.

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

모범 사례

무선 구성에 대한 모범 사례는 다음과 같습니다.

- **무선 클라이언트 fast-ssid-change** 명령을 사용하여 고속 SSID 변경을 구성합니다.
- 비밀번호 **암호화에 대해 passwd encryption on** 및 **passwd key obfuskate** 명령을 사용합니다.