単一スイッチの小規模なブランチ ネットワークでコンバージド アクセスを設定する

内容

概要

このドキュメントでは、小規模ブランチの単一スイッチ ネットワークでコンバージド アクセスを導入するためのサンプル設定を示します。この設定を数百または数千のブランチで使用して、設定をテスト/検証した後、ブランチ オフィス（支店/支社）にワイヤレス ネットワークを導入できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 3850 シリーズ スイッチ
- Cisco IOS バージョン 03.03.00SE 以降
- Cisco IES バージョン 1.2 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実に理解しておく必要があります。

背景説明

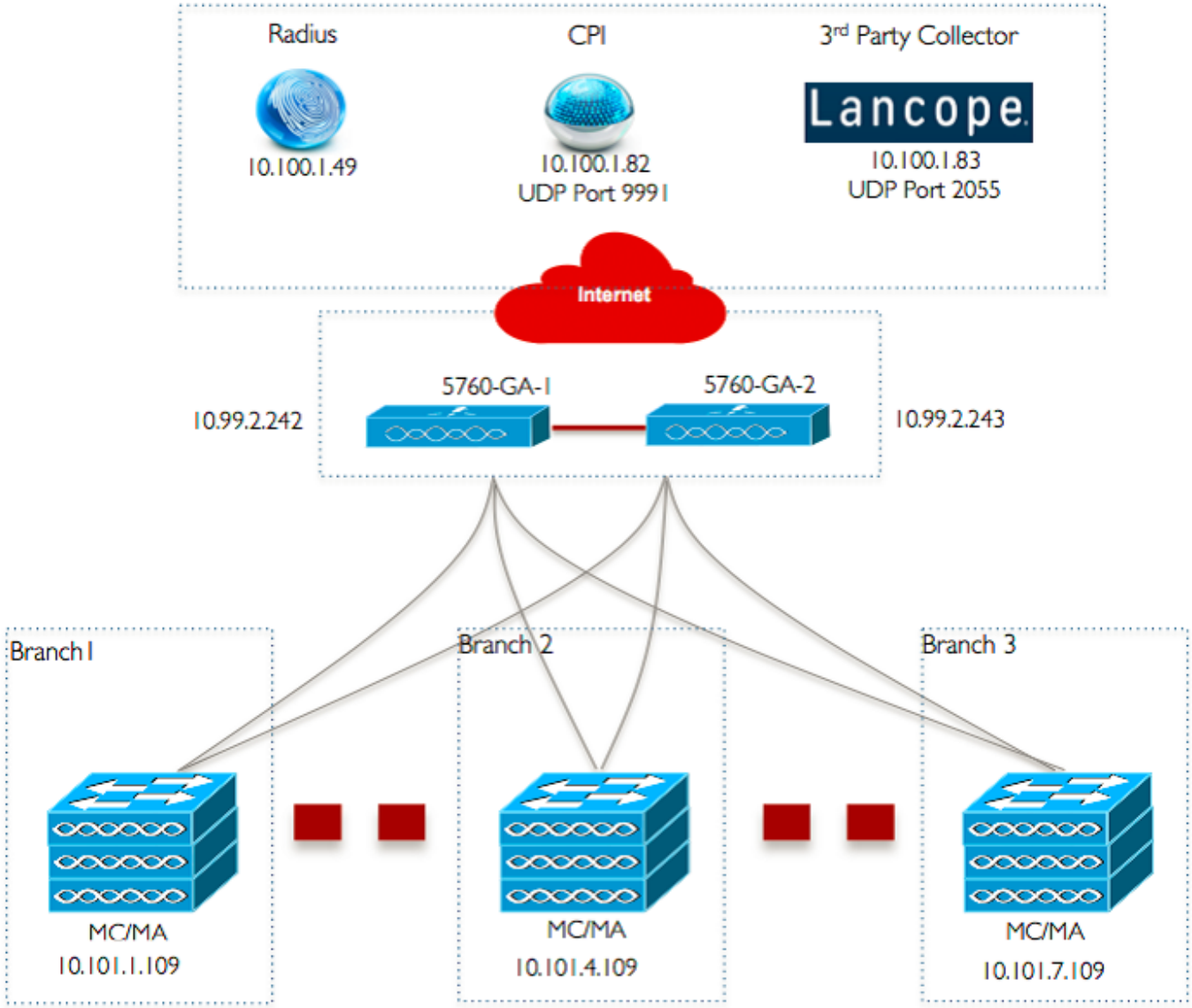
単一のイーサネット スイッチ（または複数からなるスタック）で小規模リモート ブランチ オフィスや小売店を構成することで、有線および無線ユーザにネットワーク接続を提供できます。このような小規模ネットワークでは、同じ Catalyst スイッチ上に次世代ワイヤレス機能とイーサネット スイッチングを統合できます。

このようなネットワーク設計では、ネットワーク内にスイッチ ピア グループ（SPG）などのコンバージド アクセス要素を追加せずに、ワイヤレス LAN コントローラ（WLC）のモビリティ コントローラとモビリティ エージェント（MA）の機能をスイッチで統合できます。これらのネットワークでは、ゲスト ワイヤレス サービスや、すべてのブランチ オフィスで共通するセキュリティ/ネットワーク アクセス ポリシーの適用が必要になることがあります。

設定

ネットワーク図

次の図は、一般的なブランチ ネットワークの参照トポロジを示しています。



設定

ベース レイヤ 2/3 の設定

- VLAN Trunk Protocol (VTP) モード：トランスペアレント

次に、VTP モードの設定例を示します。

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

- スパニング ツリー： Rapid-Per VLAN Spanning tree (PVST)

次の例は、Rapid-PVST 設定を示しています。

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

- **名前付き VLAN の作成**

この例では、VLAN を作成する方法を示します。

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

- **デフォルト ゲートウェイの設定**

この例では、デフォルト ゲートウェイの設定を示します。

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

- **管理 Virtual Routing and Forwarding (VRF) の設定**

この例では、管理 VRF の設定を示します。

```
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 スヌーピングの設定**

この例では、すべてのワイヤレス クライアント VLAN 用に DHCP スヌーピングが設定されます。

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

> **注：**アップリンク ポート/ポート チャネルの例に示すように、アップリンク ポートが信頼済みとマークされる必要があります。

- **Address Resolution Protocol (ARP) 検査の設定**

この例では、すべてのワイヤレス クライアント VLAN 用に ARP 検査が設定されます。

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

注：アップリンク ポート/ポート チャネルの例に示すように、アップリンク ポートが信頼済みとマークされる必要があります。

- **アップリンク ポート/ポート チャネル (必要な VLAN を許可)**

この例では、アップリンク ポート/ポート チャネルが設定されます。

```
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
```

モビリティ

- **ワイヤレス管理インターフェイス**

この例では、ワイヤレス機能が有効にされ、5760 ゲスト アンカー WLC がモビリティ ピアとして設定されます。

```
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
```

注:Cisco 5508 WLCまたは8510 AireOSをゲストアンカーコントローラとして使用できます。

セキュリティ

- **グローバル パラメータ**

この例では、グローバル パラメータの設定例を示します。

```
       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**

この例では、802.1X WLAN の設定を示します。

```
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
```

- **事前共有キー WLAN**

この例では、事前共有キー WLAN の設定を示します。

```
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**

この例では、Open WLAN の設定を示します。

```
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
```

ゲスト ソリューション

- **CWA のゲスト WLAN**

この例では、CWA のゲスト WLAN 設定を示します。

```
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 ゲスト アンカー 1 でのモビリティおよびゲスト WLAN の設定**

この例では、5760 ゲスト アンカー 1 でモビリティおよびゲスト WLAN が設定されます。

```
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
```

- **CWA (中央 Web 認証) 用の ACL のリダイレクト**

ここでは、CWA 用の ACL リダイレクトの設定例を示します。

```
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
```

高度な IOS ワイヤレス サービス

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

この例では、AVC の設定の例を示します。

```
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 設定**

この例では、WLAN の設定の例を示します。

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

- **WLAN での出力帯域幅シェーピング**

この例では、WLAN での出力帯域幅シェーピングの設定を示します。

```
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 設定**

この例では、WLAN の設定の例を示します。

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

ベスト プラクティス

ワイヤレス設定のベスト プラクティスは次のとおりです。

- wireless client fast-ssid-change コマンドを使用して高速 SSID 変更を設定します。
- **passwd encryption on および passwd key obfuscate** コマンドを使用してパスワードを暗号化します。