Configurazione dell'accesso convergente in una rete a switch singolo per piccole filiali

Sommario

Introduzione

In questo documento vengono fornite configurazioni di esempio per la distribuzione di Accesso convergente in una rete a switch singolo per filiali di piccole dimensioni. Queste configurazioni possono essere utilizzate in centinaia o addirittura in migliaia di filiali per installare la rete wireless nelle sedi distaccate con configurazioni collaudate e testate.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst serie 3850 Switch
- Cisco IOS versione 03.03.00SE o successive
- Cisco ISE versione 1.2 o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

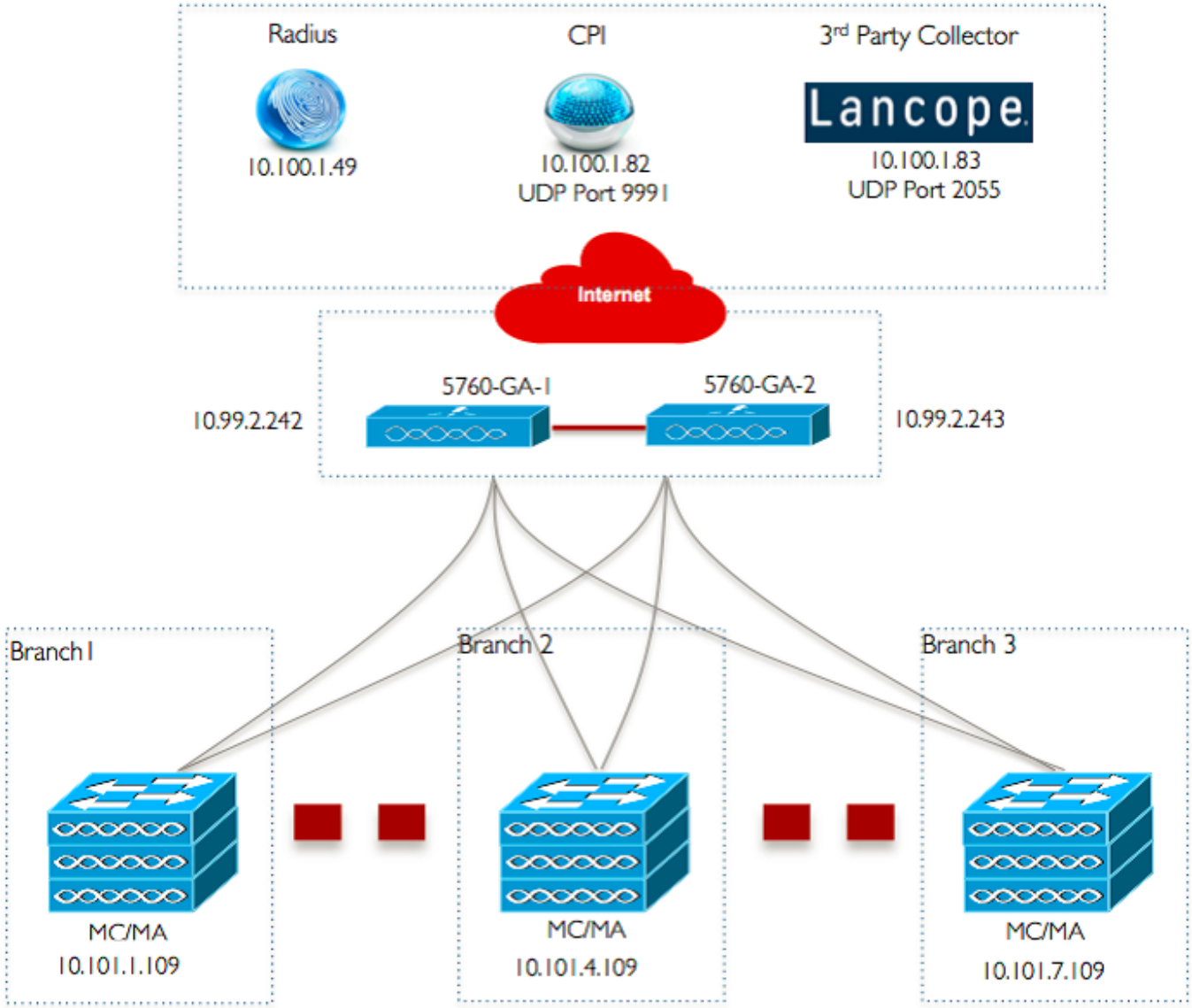
Le filiali o i punti vendita al dettaglio di piccole dimensioni possono essere costituiti da un singolo switch Ethernet o da uno stack di switch Ethernet per fornire connettività di rete agli utenti cablati e wireless. Reti di dimensioni così piccole possono far convergere la commutazione Ethernet con funzionalità wireless di nuova generazione sullo stesso switch Catalyst.

Per questo tipo di progettazione, lo switch può integrare le funzioni del controller WLC (Wireless LAN Controller) e dell'agente di mobilità (MA) senza richiedere ulteriori elementi di accesso convergente, ad esempio Switch-Peer-Group (SPG) nella rete. Queste reti possono richiedere servizi wireless guest, nonché l'applicazione di policy di sicurezza e accesso alla rete comuni a tutte le filiali.

Configurazione

Esempio di rete

In questa immagine viene illustrata una topologia di riferimento per una tipica rete di filiali.



Configurazioni

Configurazione Layer 2/3 di base

- **Modalità VLAN Trunk Protocol (VTP): Trasparente**

L'esempio mostra la configurazione della modalità VTP.

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

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

L'esempio mostra la configurazione di 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
```

- **Creazione di VLAN con nome**

Nell'esempio viene mostrato come creare le VLAN.

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

- **Configura gateway predefinito**

In questo esempio viene mostrata la configurazione del gateway predefinito.

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

- **Configurazione di VRF (Virtual Routing and Forwarding) di gestione**

In questo esempio viene illustrata la configurazione VRF di gestione.

```
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
```

- **Configurazione dello snooping DHCP IP**

Nell'esempio, lo snooping DHCP è configurato per tutte le VLAN client wireless.

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

> **Nota:** Le porte uplink devono essere contrassegnate come attendibili come mostrato nell'esempio Porte uplink/Canale porta.

- **Configura ispezione Address Resolution Protocol (ARP)**

Nell'esempio, il controllo ARP è configurato per tutte le VLAN client wireless.

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

> **Nota:** Le porte uplink devono essere contrassegnate come attendibili come mostrato nell'esempio Porte uplink/Canale porta.

- **Porte uplink/Port-Channel (consenti VLAN necessarie)**

Nell'esempio, è configurato Uplink Port/Port-Channel.

```
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
```

Mobilità

- **Interfaccia di gestione wireless**

In questo esempio, la funzionalità wireless è abilitata e il WLC 5760 Guest Anchor è configurato come peer mobilità.

```
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:è possibile usare un Cisco 5508 WLC o 8510 AireOS come controller di ancoraggio guest.

Sicurezza

- **Parametri globali**

Questo esempio mostra la configurazione dei parametri globali.

```
       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**

Nell'esempio viene mostrata la configurazione WLAN 802.1X.

```
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 a chiave già condivisa

Nell'esempio viene mostrata la configurazione della WLAN con chiave precondivisa.

```
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
```

- Apri WLAN

Nell'esempio viene mostrata la configurazione di Open WLAN.

```
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
```

Soluzione Guest

- CWA Guest WLAN

Nell'esempio viene mostrata la configurazione di CWA Guest WLAN.

```
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
```

- Configurazione di WLAN guest e mobilità su 5760 Guest Anchor 1

In questo esempio, Mobility e Guest WLAN sono configurate su 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
```

- Reindirizza ACL per CWA (Web-Auth centrale)

Nell'esempio viene mostrata la configurazione di reindirizzamento dell'ACL per CWA.

```
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
```

Servizi wireless IOS avanzati

- Configurazione di Application Visibility and Control (AVC)

Nell'esempio viene mostrata la configurazione di 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
```

- **Configurazione della WLAN**

Nell'esempio viene mostrata la configurazione della WLAN.

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

- **Bandwidth Shaping in uscita per le WLAN**

Nell'esempio viene mostrata la configurazione di Egress Bandwidth shaping per le WLAN.

```
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
```

- **Configurazione della WLAN**

Nell'esempio viene mostrata la configurazione della WLAN.

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

Procedure ottimali

Le best practice per la configurazione wireless includono:

- Uso del comando **fast-ssid-change del client wireless** per configurare la modifica rapida dell'SSID.
- L'uso dei comandi **passwd encryption on** e **passwd key offusca** per la crittografia della password.