

配置在单个交换机斯莫尔分支机构网络的聚合的访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[移动性](#)

[安全](#)

[WLAN](#)

[访客解决方案](#)

[先进的IOS无线服务](#)

[最佳实践](#)

[相关的思科支持社区讨论](#)

简介

本文为Converged在斯莫尔分组单个交换机网络的访问部署提供配置示例。这些配置可以在数百甚至千位分组间用于在有经过试验证明的配置的分支机构部署无线网络。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 3850系列交换机
- Cisco IOS版本03.03.00SE或以上
- Cisco IE版本1.2或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

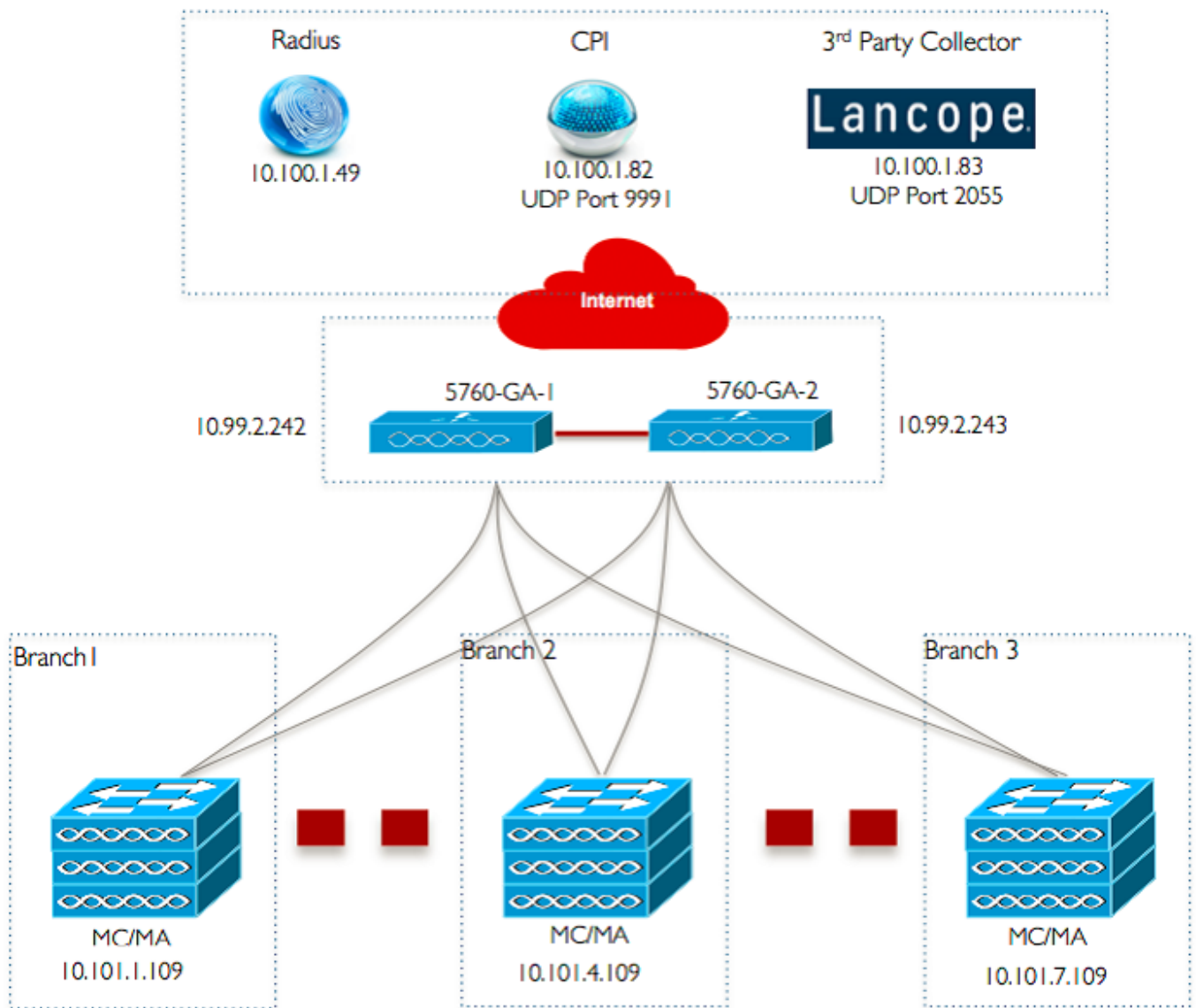
小型远程分部或零售店能包括单个或一堆栈的以太网交换机提供网络连通性给有线的和无线用户。这样小网络能聚合以太网交换以在同一台Catalyst交换机的下一代无线功能。

对于这样网络设计，交换机能集成无线局域网控制器(WLC)移动性控制器和移动性代理程序(MA)功能没有要求任何其他聚合的访问元素，例如交换机对等体组(SPG)网络的。这些网络能要求访客无线服务、以及普通的安全性和网络访问策略执行在所有分支机构间。

配置

网络图

此镜像说明一个典型的分支机构网络的一参考拓扑。



配置

基本层2/3配置

- VLAN中继协议(VTP)模式：透明
此示例显示VTP模式的配置。

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

- **生成树：急流每VLAN生成树(PVST)**

此示例显示高速PVST配置。

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

- **create命名了VLAN**

此示例显示VLAN如何创建。

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

- **配置默认网关**

默认网关配置在本例中显示。

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

- **配置管理虚拟路由和转发(VRF)**

管理VRF配置在本例中显示。

```
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
```

- **配置Ip dhcp snooping**

在本例中，监听的DHCP为所有无线客户端VLAN配置。

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

Note:必须标记如上行链路端口/Port-Channel示例所显示，上行链路端口作为信任。

- **配置地址解析服务(ARP)检查**

在本例中，ARP检查为所有无线客户端VLAN配置。

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

Note:必须标记如上行链路端口/Port-Channel示例所显示，上行链路端口作为信任。

- **上行链路端口/Port-Channel (请允许必要的VLAN)**

在本例中，上行链路端口/Port-Channel配置。

```
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
```

移动性

- 无线管理接口

在本例中，无线功能启用，并且5760访客锚点WLC配置作为移动性对等体。

```
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
```

Note:您能使用思科5508 WLC或8510 AireOS作为访客锚点控制器。

安全

- 全局参数

此示例显示全局参数的配置。

```
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

802.1X WLAN配置在本例中显示。

```
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
```

• 预先共享密钥WLAN

预先共享密钥WLAN配置在本例中显示。

```
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
```

• 打开WLAN

开放WLAN配置在本例中显示。

```
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
```

访客解决方案

• CWA访客WLAN

CWA访客WLAN配置在本例中显示。

```
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
```

- **移动性和访客在5760访客锚点1的WLAN配置**

在本例中，移动性和访客WLAN在5760访客锚点1.配置。

```
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的(中央Web-auth)重定向ACL**

重定向CWA的ACL的配置在本例中显示。

```
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
```

先进的IOS无线服务

• 应用程序可见性和控制(AVC)配置

此示例显示AVC的配置。

```
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 配置

此示例显示WLAN的配置。

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

• 出口WLAN的带宽Shaping

示例显示出口WLAN的带宽shaping的配置。

```
policy-map ABCCorp-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 配置

此示例显示WLAN的配置。

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

最佳实践

无线配置的最佳实践包括：

- 使用无线客户端法塞特ssid崔凡吉莱命令配置快速SSID更改。
- 使用密码加密和密码密钥请弄暗淡密码加密的命令。