Настройте сходившийся доступ в одном коммутаторе маленький Branch Network

Содержание

Введение

Этот документ предоставляет примеры конфигурации для Установившихся развертываний Доступа в сети одного коммутатора маленького ответвления. Эти конфигурации могут использоваться через сотни или даже тысячи ответвлений для развертывания беспроводной сети в расположениях ответвления с испытанными и протестированными конфигурациями.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Catalyst коммутатор серии 3850
- Версия Cisco IOS 03.03.00SE или позже
- Версия 1.2 IES Cisco или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

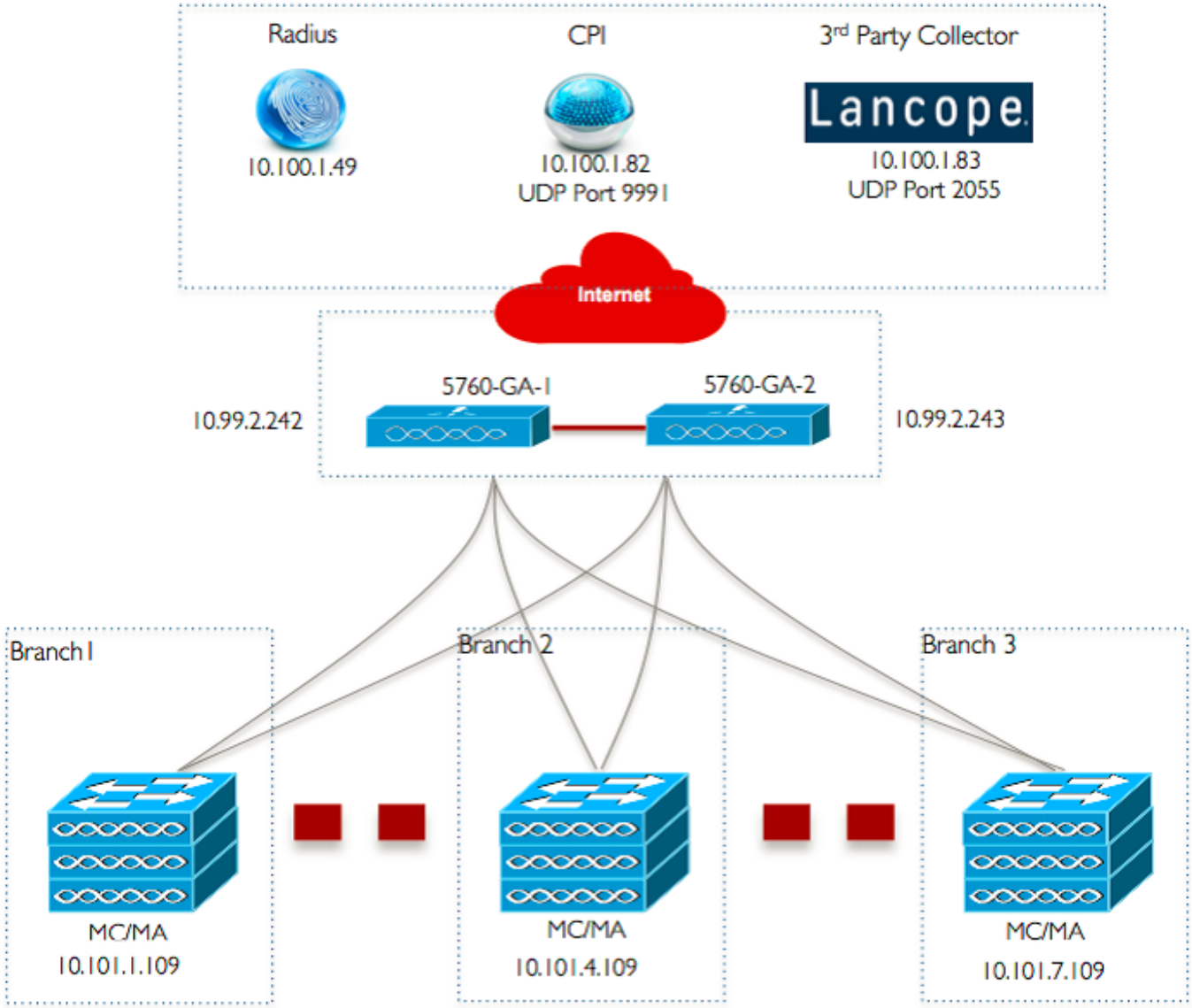
Удаленный филиал компании небольшого размера или магазин розничной торговли могут состоять из сингла или стека коммутаторов Ethernet для обеспечения сетевого подключения проводному и пользователям беспроводной связи. Такие небольшие сети могут сходиться коммутация Ethernet с поддержкой беспроводной связи следующего поколения на том же коммутаторе Catalyst.

Для таких организаций сети коммутатор может интегрировать контроллер мобильности Контроллера беспроводной локальной сети (WLC) и функции агента мобильности (MA), не требуя никаких дополнительных Установившихся элементов Доступа, таких как Группа одноранговых узлов коммутатора (SPG) в сети. Эти сети могут потребовать гостевых беспроводных сервисов, а также стандартной безопасности и принудительной политики доступа к сети через все филиалы компании.

Настройка

Схема сети

Этот образ иллюстрирует ссылочную топологию для типичного branch network.



Конфигурации

Базовый слой 2/3 Конфигурация

- **Режим транкингового протокола VLAN (VTP): прозрачный**

Данный пример показывает конфигурацию режима VTP.

```
vtp domain ‘name'



vtp mode transparent
```

- **Связующее дерево: Быстрый - На связующее дерево VLAN (PVST)**

Данный пример показывает конфигурацию 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
```

- Создайте названные VLAN

Данный пример показывает, как созданы VLAN.

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

- Настройте шлюз по умолчанию

Конфигурацию шлюза по умолчанию показывают в данном примере.

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

- Настройте виртуальную маршрутизацию менеджмента и передачу (VRF)

Конфигурацию VRF менеджмента показывают в данном примере.

```
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
```

- Настройте IP DHCP Snooping

В данном примере отслеживание DHCP настроено для всех VLAN беспроводного клиента.

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

> **Примечание:** Порты каскадного соединения должны быть отмечены столь же трастовые как показано в примере Портов/Port-channel канала от абонента к оператору.

- Настройте контроль протокола ARP

В данном примере проверка ARP настроена для всех VLAN беспроводного клиента.

```
ip arp inspection vlan 151-154,156-165
```

```
ip arp inspection validate src-mac dst-mac ip allow zeros
```

Примечание: Порты каскадного соединения должны быть отмечены столь же трастовые как показано в примере Портов/Port-channel канала от абонента к оператору.

- **Порты/Port-channel канала от абонента к оператору (позволяют необходимые VLAN),**

В данном примере/Port-Channel настроен Порт каскадного соединения.

```
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
```

Mobility

- **Интерфейс беспроводного управления**

В данном примере добавлена беспроводная функциональность, и 5760 Гостевых WLC Привязки настроены как узел мобильности.

```
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
```

Примечание: Можно использовать WLC Cisco 5508 или 8510 AireOS как контроллер абонента.

Безопасность

- **Глобальные параметры**

Данный пример показывает конфигурацию Глобальных параметров.

```
      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**

Конфигурацию WLAN 802.1X показывают в данном примере.

```
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 предварительного общего ключа

Конфигурацию WLAN Предварительного общего ключа показывают в данном примере.

```
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
```

- Открытый WLAN

Открытую конфигурацию WLAN показывают в данном примере.

```
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
```

Гостевое решение

- Гостевой WLAN CWA

Гостевую конфигурацию WLAN CWA показывают в данном примере.

```
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
```

- **Мобильность и Гостевая конфигурация WLAN на 5760 Гостевых Привязках 1**

В данном примере, Мобильности и Гостевом WLAN настроен на 5760 Гостевых Привязках 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
```

- **ACL перенаправления для CWA (центральная Веб-Аутентификация)**

Конфигурацию для перенаправления ACL для CWA показывают в данном примере.

```
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
```

Усовершенствованные беспроводные сервисы IOS

- **Видимость приложения и контроль (AVC) конфигурация**

Данный пример показывает конфигурацию 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 Configuration**

Данный пример показывает конфигурацию WLAN.

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

- **Формирование выходной пропускной способности для WLAN**

Пример показывает конфигурацию формирования Выходной пропускной способности для 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
```

- **WLAN Configuration**

Данный пример показывает конфигурацию WLAN.

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

Лучшие методы

Оптимальные методы для конфигурации беспроводной сети включают:

- Использование команды **быстрого изменения ssid беспроводного клиента** для настройки быстрого изменения SSID.
- Использование **шифрования passwd на** и **ключа passwd запутывает** команды для шифрования пароля.