

Puntos de acceso Aironet autónomos y SSID múltiples en el ejemplo de la configuración del Cisco IOS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Vídeo](#)

[Configuración AP](#)

[Paso 1. Configure el SSID y asócielo a los VLAN respectivos.](#)

[Paso 2. Asigne el cifrado a diversos SSID con los VLAN respectivos.](#)

[Paso 3. Configure la subinterfaz para la radio 0 del dot11 y los Ethernetes.](#)

[Paso 4. Verifique.](#)

[Maneje el AP con un IP Address de administración](#)

[Verificación](#)

Introducción

¿Este documento describe cómo configurar los identificadores del conjunto del servicio múltiple (SSID) con los VLAN múltiples en el Cisco IOS? software y Puntos de acceso autónomos del Cisco Aironet.

Prerrequisitos

Requisitos

Este ejemplo de configuración asume que usted ha configurado al agrupamiento DHCP en el Cisco IOS Switch o router o en un servidor DHCP dedicado.

Para completar esta configuración, Cisco recomienda que usted tiene conocimiento básico de los comandos del Cisco IOS CLI.

Componentes Utilizados

- Cualquier Switch que funcione con el Cisco IOS y soporta el Multilayer Switching (el MLS)
- Puntos de acceso del Cisco Aironet

Antecedentes

El SSID es un Identificador único que los dispositivos de la red inalámbrica utilizan para establecer y para mantener la conectividad de red inalámbrica. Los múltiples puntos de acceso en una red o un red secundario pueden utilizar los mismos SSID. Los SSID son con diferenciación entre mayúsculas y minúsculas y pueden contener hasta 32 caracteres alfanuméricos. No incluya los espacios en sus SSID.

Usted puede configurar hasta 16 SSID en su Punto de acceso del Cisco Aironet de la serie 1200 y asignar diversos ajustes de la configuración a cada SSID. Todos los SSID son activos al mismo tiempo; es decir, los dispositivos del cliente pueden asociarse al Punto de acceso usando los SSID uces de los.

Si usted quisiera que el Punto de acceso permitiera las asociaciones de los dispositivos del cliente que no especifican un SSID en sus configuraciones, usted puede configurar a un invitado SSID. El Punto de acceso incluye al invitado SSID en su faro. El SSID predeterminado del Punto de acceso, *tsunami*, se fija al modo de invitado. Sin embargo, para mantener su red segura, usted debe inhabilitar al modo de invitado SSID en la mayoría de los Puntos de acceso.

Si su Punto de acceso es un repetidor o es una punta de acceso a raíz que actúa como padre para un repetidor, usted puede configurar un SSID para el uso en el modo repetidor. Usted puede asignar un nombre de usuario de autenticación y una contraseña al modo repetidor SSID para permitir que el repetidor autentique a su red como un dispositivo del cliente.

Si sus VLA N de los usos de la red, usted pueden asignar un SSID a un VLA N. Los dispositivos del cliente que utilizan el SSID se agrupan en ese VLA N.

Vídeo

Este vídeo muestra la configuración descrita en este documento:

Configuración AP

Esta configuración utiliza los VLA N (1, 2, y 3) con el natural como V: LAN1 y asignación a 3 diversos SSID (UNO, DOS, y TRES) en cualquier Punto de acceso del Cisco Aironet.

- El SSID UNO utiliza la encriptación WEP.
- Aplicaciones WPA-PSK SSID DOS.
- Aplicaciones WPA-2-PSK SSID TRES.
- Si se asume que el acceso de Ethernet AP está conectada con el puerto fa 2/1 del Switch.
- Transmitir los 3 SSID.
- Si usted utiliza un solo SSID, utilice el comando del **modo de invitado** bajo el SSID.
- Si usted utiliza los SSID múltiples, utilice el comando del **mbssid** bajo el SSID y bajo interfaces radio

Nota: El modo de invitado reemplaza SSID básico múltiple (MBSSID).

Complete estos pasos para configurar el AP:

Paso 1. Configure el SSID y asócielo a los VLAN respectivos.

```
Enable
Conf t
Dot11 ssid one
Vlan 1
Authentication open
Mbssid Guest-mode
End
```

```
Enable
Conf t
Dot11 ssid two
Vlan 2
authentication open
authentication key-management wpa
wpa-psk ascii 7
Mbssid Guest-mode
End
```

```
Enable
Conf t
Dot11 ssid three
Vlan 3
authentication key-management wpa version 2
wpa-psk ascii 7
Mbssid Guest-mode
End
```

Paso 2. Asigne el cifrado a diversos SSID con los VLAN respectivos.

```
Enable
Int dot11 0
Mbssid
ssid one
ssid two
ssid three

encryption vlan 1 mode wep mandatory
encryption vlan 1 key 1 size 40bit
encryption vlan 2 mode ciphers tkip
encryption vlan 3 mode ciphers aes-ccm
```

Paso 3. Configure la subinterfaz para la radio 0 del dot11 y los Ethernetes.

En el AP:

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# bridge group 1
```

```
AP(config-subif)# interface FastEthernet0.1
AP(config-subif)# bridge group 1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# end
AP# write memory
```

```
AP(config)# interface Dot11Radio0.2
AP(config-subif)# encapsulation dot1Q 2
AP(config-subif)# bridge group 2
```

```
AP(config-subif)# interface FastEthernet0.2
AP(config-subif)# bridge group 2
AP(config-subif)# encapsulation dot1Q 2
AP(config-subif)# end
AP# write memory
```

```
AP(config)# interface Dot11Radio0.3
AP(config-subif)# encapsulation dot1Q 3
AP(config-subif)# bridge group 3
```

```
AP(config-subif)# interface FastEthernet0.3
AP(config-subif)# bridge group 3
AP(config-subif)# encapsulation dot1Q 3
AP(config-subif)# end
AP# write memory
```

```
AP(config)# bridge irb
Ap(config)# bridge 1 route ip
Ap(config)# end
Ap# wr
```

En el switch:

```
en
conf t
int fa 2/1
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,2,3
end
```

Paso 4. Verifique.

- En el AP, utilice el comando **show dot11 associations**. Usted debe ver los 3 SSID.

```
ap#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [one] :
SSID [two] :
SSID [three] :
```

- Haga ping del AP a la interfaz VLAN del Switch. Usted debe poder hacer ping.

Maneje el AP con un IP Address de administración

Asigne la dirección IP al (BVI) del Interfaz Virtual de Bridge del AP:

```
Enable
Conf t
Int bvi 1
Ip address
No shut
End
```

Verificación

Utilice el comando del **Br del IP internacional de la demostración** en el AP, y verifíquelo que todas las interfaces son en servicio.