

Configurando o link de malha ponto a ponto com ponte Ethernet em APs Mobility Express

Contents

[Introdução](#)

[Sobre o Mobility Express](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configuração](#)

[Configurações do switch](#)

[Redefinição de fábrica dos APs](#)

[Baixando a imagem do Lightweight Capwap para 1542-2 \(MAP\)](#)

[Download da imagem compatível com o Mobility Express para AP 1542-1 \(RAP\)](#)

[Provisionamento de SSID de dia zero](#)

[Configuração de malha adicional](#)

[Verificar](#)

[Troubleshooting](#)

[Dicas, truques e erros comuns](#)

Introdução

Este documento descreve o processo de implantação de links de malha ponto-a-ponto com Ethernet Bridging usando o software Cisco Mobility Express (ME).

Sobre o Mobility Express

Este documento usa Pontos de Acesso Cisco 1542 externos. O suporte em malha do software Mobility Express para APs internos e externos no modo Flex+Bridge foi introduzido na versão 8.10.

Os seguintes modelos de AP são suportados:

- Como um AP raiz ME: APs Cisco AireOS 1542, 1562, 1815s, 3802s
- Como um AP em malha: APs Cisco AireOS 1542, 1562, 1815s, 3802s

O Mobility Express (ME) é uma solução que substitui o modo e o software do AP Autônomo. Ele permite que uma versão mais leve do software Wireless LAN Controller (WLC) baseado no AireOS seja executada no próprio Ponto de acesso. O código da WLC e do AP é armazenado em uma única partição da memória do AP. Uma implantação do Mobility Express não requer um arquivo de licença, nem ativação de licença.

Quando o dispositivo que executa o software com capacidade para Mobility Express é ligado, a "parte do AP" é inicializada primeiro. Alguns minutos mais tarde, a parte do controlador também é inicializada. Uma vez estabelecida uma sessão de console, um dispositivo habilitado para ME mostrará o prompt da WLC. Para entrar no shell de AP subjacente, um comando `apciscoshell` pode ser usado:

```
<#root>
```

```
(Cisco Controller) >
```

```
apciscoshell
```

```
!!Warning!!: You are entering ap shell. This will stop you from establishing new telnet/SSH/Web session.  
Also the existing sessions will be suspended till you exit the ap shell.  
To exit the ap shell, use 'logout'
```

```
User Access Verification
```

```
Username:
```

```
admin
```

```
Password:
```

```
*****
```

```
RAP>
```

```
logout
```

```
(Cisco Controller) >
```

Pré-requisitos

Componentes Utilizados

- 2x access points 1542D-E
- 2 switches Cisco 3560-CX
- 2x notebooks
- 1x Cabo de Console

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

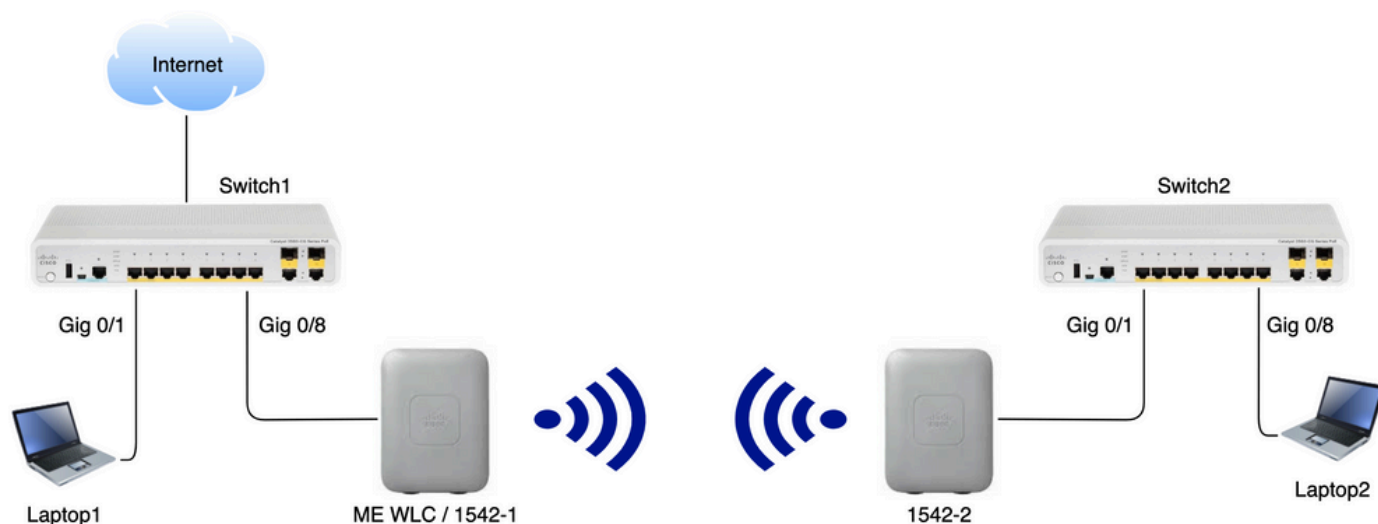
Diagrama de Rede

Todos os dispositivos nessa rede estarão localizados dentro da sub-rede 192.168.1.0/24. O AP (controlador) do Mobility Express terá sua interface de gerenciamento não marcada, enquanto a VLAN nativa em todas as portas será a VLAN 39. O AP 1542-1 assumirá a função de controlador

e de ponto de acesso raiz (RAP), enquanto o AP 1542-2 assumirá a função de ponto de acesso em malha (MAP). Esta tabela contém os endereços IP de todos os dispositivos na rede:

Observação: marcar a interface de gerenciamento pode causar problemas com o AP que ingressa no processo interno da WLC. Se você decidir marcar a interface de gerenciamento, certifique-se de que a parte da infraestrutura com fio esteja configurada de acordo.

Dispositivo	IP Address
Gateway padrão	192.168.1.1
Notebook 1	192.168.1.100
Notebook 2	192.168.1.101
WLC Mobility Express	192.168.1.200
1542-1 (RAP)	192.168.1.201
1542-2 (MAPA)	192.168.1.202



Configuração

Configurações do switch

As portas de switch onde os laptops estão conectados são configuradas como portas de acesso com a VLAN definida como 39:

```
<#root>
```

```
switch1
```

```
#show run interface Gig 0/1
```

```
Current configuration : 205 bytes
```

```
!
```

```
interface GigabitEthernet0/1
```

```
description Laptop1
```

```
switchport access vlan 39
```

```
switchport mode access
end
```

```
<#root>
```

```
switch2
```

```
#show run interface Gig 0/8
```

```
Current configuration : 205 bytes
```

```
!
```

```
interface GigabitEthernet0/8
```

```
description Laptop2
```

```
switchport access vlan 39
```

```
switchport mode access
```

```
end
```

As portas de switch onde os APs estão conectados estarão no modo de tronco com a VLAN nativa definida como 39:

```
<#root>
```

```
switch1
```

```
#show run interface Gig 0/8
```

```
Building configuration...
```

```
!
```

```
interface GigabitEthernet0/8
```

```
description 1542-1 (RAP)
```

```
switchport mode trunk
```

```
switchport trunk native vlan 39
```

```
end
```

```
<#root>
```

```
switch2
```

```
#show run interface Gig 0/1
```

```
Building configuration...
```

```
!
```

```
interface GigabitEthernet0/1
```

```
description 1542-1 (RAP)
```

```
switchport mode trunk
```

```
switchport trunk native vlan 39
```

```
end
```

Redefinição de fábrica dos APs

É recomendável executar uma redefinição de fábrica dos APs antes de iniciar uma nova implantação. Isso pode ser feito pressionando o botão mode/reset no AP, conectando a energia e

mantendo-a pressionada por mais de 20 segundos. Isso garantirá que todas as configurações anteriores tenham sido apagadas. O AP poderá ser acessado através de uma conexão de console com o nome de usuário padrão Cisco e a senha Cisco (diferencia maiúsculas de minúsculas).

Uma redefinição de fábrica não necessariamente move um AP de volta para o modo lightweight se ele já estiver sendo executado no Mobility Express. Uma etapa importante é identificar se seus APs estão executando uma imagem leve ou uma imagem expressa do Mobility.

Se o seu AP for leve, você poderá convertê-lo para o Mobility Express fazendo o download do código do Mobility Express. Se o AP já estiver no modo Mobility Express, você terá que seguir o processo de atualização na GUI do access point/controlador para alterar a versão do software.

Exemplo de um show version do AP executando imagem lightweight :

```
cisco AIR-AP1562I-E-K9 ARMv7 Processor rev 1 (v7l) with 1028616/605344K bytes of memory. Processor board ID FCZ2150Z099 AP
Running Image : 8.5.151.0 Primary Boot Image : 8.5.151.0 Backup Boot Image : 0.0.0.0 1 Gigabit Ethernet interfaces 2 802.11 Radios Radio
Driver version : 9.0.5.5-W8964 Radio FW version : 9.1.8.1 NSS FW version : 2.4.26
```

Este é um exemplo de AP já em execução no software Mobility Express :

```
AP#show version ... AP Running Image : 8.10.185.0 Primary Boot Image : 8.10.185.0 Backup Boot Image : 8.10.185.0 ... AP Image type :
MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE
```

Baixando a imagem do Lightweight Capwap para 1542-2 (MAP)

O Laptop 1 será usado como um servidor TFTP. O AP 1542-2 pode ser inicialmente conectado à porta 1 Gig 0/8 do Switch apenas para que a atualização possa ser realizada. Em software.cisco.com, em 1542 imagens lightweight, faça o download de 15.3.3-JJ1 (nome completo ap1g5-k9w8-tar.153-3.JK9.tar) que corresponde à imagem da versão 8.10.185. A imagem mais recente do AP leve sempre corresponderá à versão mais recente do ME. Coloque a imagem na pasta raiz do TFTP. Conecte o cabo do console, faça login usando as credenciais padrão (o nome de usuário é Cisco e a senha também é Cisco). Atribua o endereço IP ao AP e execute a atualização usando os seguintes comandos:

```
#capwap ap ip 192.168.1.202 255.255.255.0 192.168.1.1
#archive download-sw /reload tftp://192.168.1.100/ap1g5-k9w8-tar.153-3.JK9.tar
```

O AP executará a atualização e, em seguida, reiniciará. Confirme se a atualização foi bem-sucedida usando o comando show version:

```
<#root>
```

```
MAP#
```

```
show version
```

.
..
AP Running Image : 8.10.185.0
Primary Boot Image : 8.10.185.0
Backup Boot Image : 8.8.125.0

O AP será desconectado do Switch 1 e conectado novamente ao Switch 2.

Observação: ao atualizar a imagem do MAP manualmente, evitamos que o processo de atualização da imagem ocorra no ar quando o link de malha for estabelecido.

Download da imagem compatível com o Mobility Express para AP 1542-1 (RAP)

Em Mobility Express 8.10.105 releases para 1542 AP, podemos ver 2 arquivos disponíveis: .tar e .zip. Faça o download do arquivo .tar

Aironet 1542I Outdoor Access Point

Release 8.10.185.0 [My Notifications](#)

[Related Links and Documentation](#)
[Release Notes for 8.10.185.0](#)

File Information	Release Date	Size	
Cisco 1540 Series Mobility Express Release 8.10 Software, to be used for conversion from Lightweight Access Points only. AIR-AP1540-K9-ME-8-10-185-0.tar Advisories	24-Mar-2023	60.80 MB	
Cisco 1540 Series Mobility Express Release 8.10 Software. Access Point image bundle, to be used for software update and/or supported access points images. AIR-AP1540-K9-ME-8-10-185-0.zip Advisories	24-Mar-2023	503.27 MB	

Faça o download do arquivo .tar

Diferentemente de uma WLC física, os pontos de acesso ME não têm memória flash suficiente para armazenar todas as imagens de AP, portanto, ter um servidor TFTP acessível o tempo todo é necessário se você quiser unir mais APs ao seu ponto de acesso Mobility Express. Esta etapa não é necessária se atualizarmos manualmente os APs como neste exemplo.

Para executar a atualização, conecte o console ao AP 1542-1, atribua um endereço IP a ele e execute a atualização da imagem:

```
#capwap ap ip 192.168.1.201 255.255.255.0 192.168.1.1  
#ap-type mobility-express tftp://192.16.1.100/AIR-AP1540-K9-ME-8-10-185.tar
```

Quando a atualização for concluída, o AP será reinicializado. Logo após o AP estar ativado, a parte controladora também começa a ser inicializada. Logo veremos o SSID de provisionamento de dia zero "CiscoAirProvision" sendo transmitido.

Se estiver no console, você pode ver um assistente CLI, mas não configure o AP dessa maneira. O assistente de GUI por satélite é o caminho a seguir.

Provisionamento de SSID de dia zero

Conecte-se ao SSID "CiscoAirProvision" transmitido pelo AP usando a senha password. O laptop obtém um endereço IP da sub-rede 192.168.1.0/24.

Caso você não veja o SSID sendo transmitido, ainda é possível que o AP esteja em "Mobility express CAPABLE", mas não esteja sendo executado como mobility express. Em seguida, você teria que se conectar à CLI do AP e digitar `ap type mobility-express` e o AP reinicializa e transmite o SSID de provisionamento.

Também é possível converter o AP entre o modo local e o modo de malha usando "capwap ap mode local/flex-bridge", se necessário, durante essa configuração.

Abra o endereço <http://192.168.1.1> em um navegador da Web. Esta página redireciona para o assistente de configuração inicial. Crie uma conta de administrador no controlador especificando o nome de usuário e a senha do administrador e, em seguida, clique em Iniciar.



Cisco Aironet 1542 Series Mobility Express

Welcome! Please start by creating an admin account.

The same credentials will be used for Access Point
SSH login.

Na próxima etapa, configure o controlador especificando os valores.

Nome do campo	Descrição
Nome do sistema	Digite o nome do sistema para o AP do Mobility Express. Exemplo: MobilityExpress-WLC
País	Escolha um país na lista suspensa.

Data e hora	<p>Escolha a data e a hora atuais.</p> <p>Observação: o assistente tenta importar as informações de relógio (data e hora) do computador usando JavaScript. É altamente recomendável que você confirme as configurações do relógio antes de continuar. Os pontos de acesso dependem das configurações do relógio para se unirem à WLC.</p>
Fuso horário	Escolha o fuso horário atual.
Servidor NTP	Insira os detalhes do servidor NTP.
IP de gerenciamento	<p>Insira o endereço IP de gerenciamento.</p> <p>OBSERVAÇÃO: ele deve ser diferente do IP atribuído ao ponto de acesso! Neste exemplo, enquanto o AP obteve o IP .201, atribuímos .200 no assistente de configuração. ambos serão usados.</p>
Máscara de sub-rede	Digite o endereço da máscara de sub-rede.
Gateway padrão	Insira o gateway padrão.

Nessa configuração, o servidor DHCP será executado no Switch 1, portanto não há necessidade de ativá-lo no ME WLC. Deslize a opção Malha para Enable e clique em Avançar.



1 Set Up Your Controller

System Name ?

Country ?

Date & Time

Timezone ?

NTP Server ?

Enable IP Management(Management Network) ?

Management IP Address ?

Subnet Mask

Default Gateway


Mesh


Enable DHCP Server (Management Network)

Na próxima etapa, crie a rede sem fio especificando os seguintes campos:

Nome do campo	Descrição
Nome da rede	Digite o nome da rede.
Security	Escolha o Tipo de segurança WPA2 Personal na lista suspensa.
Senha	Especifique a chave pré-compartilhada (PSK).
Confirmar senha	Insira novamente e confirme a frase secreta.

Esta rede pode ser desativada em um estágio posterior.

 Cisco Aironet 1542 Series Mobility Express


1 Set Up Your Controller 


>


2 Create Your Wireless Networks

∨

Employee Network

Network Name 

Security 

Passphrase 

Confirm Passphrase

Na guia Configurações avançadas, deixe o botão Otimização de Parâmetros de RF desabilitado e clique em Avançar



Cisco Aironet 1542 Series Mobility Express

1 Set Up Your Controller 



2 Create Your Wireless Networks



3 Advanced Setting



RF Parameter Optimization

Back

Next

Quando as configurações forem confirmadas, a WLC será reiniciada:



The controller has been fully configured and will restart in 60 seconds.

Next Steps:

After the controller is restarted, it will be accessible from the network by going to this URL -

<https://192.168.1.200>

1 Controller Settings

Username	admin
System Name	ME
Country	Netherlands (NL)
Date & Time	11/05/2019 10:31:39
Timezone	Amsterdam, Berlin, Rome, Vienna
NTP Server	-
Management IP Address	192.168.1.200
Management IP Subnet	255.255.255.0
Management IP Gateway	192.168.1.1
Mesh	Yes

x Controller DHCP

2 Wireless Network Settings

✓ Employee Network

Network Name	Employee
Security	WPA2 Personal
Passphrase:	*****

Configuração de malha adicional

Antes de estabelecer o enlace de malha, o MAP precisa ser convertido no modo de ponte flexível. O RAP já estará no modo flex-bridge se a opção mesh tiver sido habilitada durante a configuração inicial. Isso pode ser feito no CLI:

```
<#root>
```

```
MAP#
```

```
capwap ap mode flex-bridge
```

MAP#[*11/05/2019 18:26:28.1599] AP Rebooting: Reset Reason - AP mode changed

Para que o MAP top se una à controladora ME, ele precisa ser autorizado. No MAP, localize o endereço mac de sua interface ethernet:

<#root>

MAP#

```
show interfaces wired 0
```

```
wired0    Link encap:Ethernet  HWaddr
```

```
00:EE:AB:83:D3:20
```

```
inet addr:192.168.1.202  Bcast:192.168.1.255  Mask:255.255.255.0
UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
RX packets:183 errors:0 dropped:11 overruns:0 frame:0
TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:80
RX bytes:19362 (18.9 KiB)  TX bytes:22536 (22.0 KiB)
```

No laptop 1, acesse a interface da Web do controlador ME via <https://192.168.1.200>. Após a ativação do modo especialista (canto superior direito), uma guia de malha será exibida em Wireless settings (Configurações sem fio). Em mac filtering (filtragem MAC), adicione o endereço MAC Ethernet do MAP:

The screenshot shows the Cisco Aironet 1542 Series Mobility Express web interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (with sub-items: WLANs, Access Points, Access Points Groups, WLAN Users, Guest WLANs, DHCP Server, and Mesh), Management, Services, and Advanced. The 'Mesh' option is highlighted with a red box. The main content area is titled 'Mesh settings' and features a 'Mesh' button. Below this, there are tabs for 'General', 'Mesh RAP Downlink backhaul', 'Convergence', 'Ethernet bridging', 'Security', and 'MAC Filtering', with 'MAC Filtering' selected and highlighted by a red box. The 'MAC Filtering' page includes a search bar, an 'Add MAC Address' button, a 'Refresh' button, and a table with columns for 'MAC Address', 'Type', 'Profile Name', and 'Description'. The table currently shows 'Number of Blacklist:0' and 'Number of Whitelist:0'.



Add MAC Address

MAC Address

00:EE:AB:83:D3:20

Description

MAP



Type

WhiteList



Profile Name

Any WLAN/RLAN



Apply

Cancel

Observação: qualquer AP subsequente no modo bridge ou flex-bridge que esteja sendo adicionado ao ME WLC também precisa ser autorizado

Após a configuração, um enlace de malha deve ser estabelecido. Para que o cliente com fio por trás do MAP passe o tráfego pelo link de malha, o Ethernet Bridging precisa ser habilitado no MAP em Wireless Settings > Access Points > MAP > Mesh:

Cisco Aironet 1542 Series Mobility Express

ACCESS POINTS ADMINISTRATION

Access Points 1

Q Search

Refresh

Select	Manage	Type	Location
<input type="checkbox"/>		ME Capable	default location

10 Items per page

RAP(Active Controller)

General Controller Radio 1 (2.4 GHz) Radio 2 (5GHz) Mesh

AP Role: Root

Bridge Type: Outdoor

Bridge Group Name:

Strict Matching BGN:

Daisy Chaining:

Preferred Parent:

Backhaul Interface: 802.11a/n/ac

Bridge Data Rate (Mbps): auto

Install Mapping on Radio Backhaul:

Ethernet Link Status: UP

PSK Key TimeStamp: Delete PSK

Mesh RAP Downlink backhaul

5 GHz 2.4 GHz

Ethernet Bridging

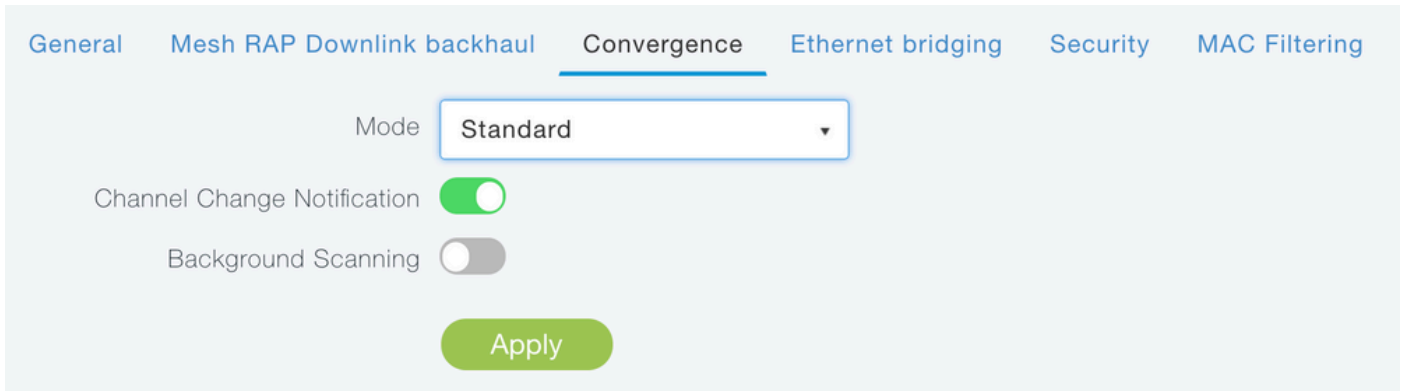
State

Acti...	Interface Name	Oper Status	Mode	VLAN Id
<input type="checkbox"/>	GigabitEthernet0	UP	Access	0

1 - 1 of 1 items

Apply Cancel

Se o link de malha estiver usando uma banda de 5 GHz, ele pode ser afetado por assinaturas de radar. Uma vez que o RAP detecta um evento de radar, ele vai mudar para outro canal. É recomendável habilitar a Notificação de Alteração de Canal para que o RAP notifique o MAP de que o canal será comutado. Isso reduz significativamente o tempo de convergência, pois o MAP não precisa verificar todos os canais disponíveis:



Verificar

Podemos verificar se o MAP ingressou executando o comando `show mesh ap summary`:

```
<#root>
```

```
(Cisco Controller) >
```

```
show mesh ap summary
```

AP Name	AP Model	BVI MAC	CERT MAC	Hop	Bridge Group Name
RAP	AIR-AP1542I-E-K9	00:fd:22:19:8c:f8	11:22:33:44:55:66	0	default
MAP	AIR-AP1542D-E-K9	00:ee:ab:83:d3:20	11:22:33:44:55:66	1	default

```
Number of Mesh APs..... 0
Number of RAPs..... 0
Number of MAPs..... 0
Number of Flex+Bridge APs..... 2
Number of Flex+Bridge RAPs..... 1
Number of Flex+Bridge MAPs..... 1
```

Para testar se o link está passando pelo tráfego, tentaremos fazer ping do Laptop 1 para o Laptop 2:

```
<#root>
```

```
VAPEROVI:~ vaperovi$
```

```
ping 192.168.1.101
```

```
PING192.168.1.101 (192.168.1.101): 56 data bytes
64 bytes from192.168.1.101: icmp_seq=0 ttl=64 time=5.461 ms
64 bytes from192.168.1.101: icmp_seq=1 ttl=64 time=3.136 ms
64 bytes from192.168.1.101: icmp_seq=2 ttl=64 time=2.875 ms
```

Observação: você só poderá fazer ping no endereço IP do MAP ou do RAP depois que o

link de malha tiver sido estabelecido.

Troubleshooting

No MAP/RAP:

- debug mesh events

No WLC ME:

- debug capwap events enable
- debug capwap errors enable
- debug mesh events enable

Exemplo de um processo de junção bem-sucedido observado no MAP (algumas mensagens foram redigidas, pois não são relevantes):

<#root>

MAP#debug mesh events

Enabled all mesh event debugs

[*11/05/2019 18:28:24.5699] EVENT-MeshRadioBackhaul[1]: Sending SEEK_START to Channel Manager

[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]:

Starting regular seek

[*11/05/2019 18:28:24.5699] EVENT-MeshChannelMgr[1]: channels to be sought: 100

[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[0]: start scanning on channel 1.

[*11/05/2019 18:28:06.5499] EVENT-MeshChannelMgr[1]: start scanning on channel 100.

[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADD_LINK to MeshLink

[*11/05/2019 18:28:06.5699] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: AWPP adjacency added channel(100)

[*11/05/2019 18:28:06.5699] EVENT-MeshRadioBackhaul[1]: Sending ADJ_FOUND to Channel Manager 0x64

[*11/05/2019 18:28:06.5699] EVENT-MeshChannelMgr[1]: Adj found on channel 100.

[*11/05/2019 18:28:07.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:08.5499] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[0]: continue scanning on channel 2.

[*11/05/2019 18:28:08.7899] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:09.0399] EVENT-MeshChannelMgr[1]: continue scanning on channel 104.

[*11/05/2019 18:28:09.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:10.7899] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:11.0199] EVENT-MeshChannelMgr[0]: continue scanning on channel 3.

[*11/05/2019 18:28:11.0399] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:11.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:11.3099] EVENT-MeshChannelMgr[1]: continue scanning on channel 108.

[*11/05/2019 18:28:13.0199] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:13.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:13.2499] EVENT-MeshChannelMgr[0]: continue scanning on channel 4.

[*11/05/2019 18:28:13.3099] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:13.5599] EVENT-MeshChannelMgr[1]: continue scanning on channel 112.

[*11/05/2019 18:28:15.2099] ipv6 gw config loop in Ac discovery

[*11/05/2019 18:28:15.2499] EVENT-MeshChannelMgr[0]: scanning timer expires.

[*11/05/2019 18:28:15.5099] EVENT-MeshChannelMgr[0]: continue scanning on channel 5.

[*11/05/2019 18:28:15.5599] EVENT-MeshChannelMgr[1]: scanning timer expires.

[*11/05/2019 18:28:15.8099] EVENT-MeshChannelMgr[1]: continue scanning on channel 116.

```
.
..
.
[*11/05/2019 18:28:35.7999] EVENT-MeshChannelMgr[1]: Mesh BH requests to switch to channel 100, width 20 MHz
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: abort scanning.
[*11/05/2019 18:28:35.8199] EVENT-MeshChannelMgr[0]: Set to configured channel 1, width 20 MHz
[*11/05/2019 18:28:36.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:37.5099] EVENT-MeshRadioBackhaul[1]: Sending LINK_UP to MeshLink
[*11/05/2019 18:28:37.5099] CRIT-MeshLink: Set Root port Mac: D4:78:9B:7B:DF:11 BH Id: 2 Port:54 Device:DEV
[*11/05/2019 18:28:37.5099] EVENT-MeshLink: Sending NOTIFY_SECURITY_LINK_UP to MeshSecurity
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Intermodule message NOTIFY_SECURITY_LINK_UP
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: Start full auth to parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:37.5099] EVENT-MeshSecurity: start_auth, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: Opening wpas socket
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: start socket to WPA supplicant
[*11/05/2019 18:28:37.5199] EVENT-MeshSecurity: MeshSecurity::wpas_init my_mac=00:EE:AB:83:D3:20, user=
[*11/05/2019 18:28:38.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6699] ipv6 gw config loop in Ac discovery
[*11/05/2019 18:28:40.6799] EVENT-MeshSecurity: Generating pmk r0 as child(D4:E8:80:A0:D0:B1)
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: pmk(eap) r0 generated for D4:78:9B:7B:DF:11: 5309c9fb0c1e1e1e1e1e1e1e1e1e1e1e
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: EAP authentication is done, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Child(D4:E8:80:A0:D0:B1) generating keys to Parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_AUTH_RSP, Parent(D4:78:9B:7B:DF:11) state changed to STATE_AUTH
[*11/05/2019 18:28:40.6899] CRIT-MeshSecurity: Mesh Security successful authenticating parent D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mac: D4:78:9B:7B:DF:11 bh_id:2 auth_result: 1
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Sending NOTIFY_SECURITY_DONE to Control
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Mesh Link:Security success on parent :D4:78:9B:7B:DF:11
[*11/05/2019 18:28:40.6899] EVENT-MeshLink: Uplink Auth done: Mac: D4:78:9B:7B:DF:11 Port:54 Device:DEV
[*11/05/2019 18:28:40.6899] EVENT-MeshSecurity: Processing TGR_REASSOC_RSP, Parent(D4:78:9B:7B:DF:11)
```

state changed to STATE_RUN

```
[*11/05/2019 18:28:40.6899] EVENT-MeshAwppAdj[1][D4:78:9B:7B:DF:11]: auth_complete Result(PASS)
```

```
.
..
.
[*11/05/2019 18:28:45.6799] CAPWAP State: Discovery
[*11/05/2019 18:28:45.6799] Discovery Request sent to 192.168.1.200, discovery type STATIC_CONFIG(1)
[*11/05/2019 18:28:45.6899] Discovery Request sent to 192.168.1.200, discovery type STATIC_CONFIG(1)
[*11/05/2019 18:28:45.6899] Sent Discovery to mobility group member 1. 192.168.1.200, type 1.
[*11/05/2019 18:28:45.7099] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)
[*11/05/2019 18:28:46.9699] AP GW IP Address updated to 192.168.1.1
[*11/05/2019 18:28:47.3999] Flexconnect Switching to Standalone Mode!
[*11/05/2019 18:28:47.4599] EVENT-MeshLink: Sending NOTIFY_CAPWAP_COMPLETE to Control
[*11/05/2019 18:28:47.4599] EVENT-MeshControl: Capwap Complete Notification: bh:2 Result:2
[*11/05/2019 18:28:47.4599] EVENT-MeshControl: Received CAPWAP Disconnect for: bh_id(2), D4:78:9B:7B:DF:11
[*11/05/2019 18:28:47.4899]
```

Discovery Response from 192.168.1.200

```
.
..
.
Adding Ipv4 AP manager 192.168.1.200 to least load
[*11/05/2019 18:28:55.1299] WLC: ME ApMgr count 1, ipTransportTried 0, prefer-mode 1, isIpv4orIpv6Static 1
[*11/05/2019 18:28:55.1399] IPv4 Pref mode. Choosing AP Mgr with index 0, IP 192.168.1.200, load 1, AP Mgr Count 1
[*11/05/2019 18:28:55.1399] capwapSetTransportAddr returning: index 0, apMgrCount 0
[*11/05/2019 18:28:55.1399]
[*11/06/2019 13:23:36.0000]
[*11/06/2019 13:23:36.0000] CAPWAP State: DTLS Setup
[*11/06/2019 13:23:36.0000] DTLS connection created successfully local_ip: 192.168.1.202 local_port: 5246
[*11/06/2019 13:23:36.8599] Dtls Session Established with the AC 192.168.1.200, port 5246
```

```

[*11/06/2019 13:23:36.8599]
[*11/06/2019 13:23:36.8599] CAPWAP State: Join
[*11/06/2019 13:23:36.8699] Sending Join request to 192.168.1.200 through port 5248
[*11/06/2019 13:23:36.8899] Join Response from 192.168.1.200
[*11/06/2019 13:23:36.8899] AC accepted join request with result code: 0
.
..
.
CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:37.4999] Starting Post Join timer
[*11/06/2019 13:23:37.4999]
[*11/06/2019 13:23:37.4999] CAPWAP State: Image Data
[*11/06/2019 13:23:37.5099] AP image version 8.10.105.0 backup 8.8.125.0, Controller 8.10.105.0
[*11/06/2019 13:23:37.5099] Version is the same, do not need update.
[*11/06/2019 13:23:37.6399] do NO_UPGRADE, part1 is active part
[*11/06/2019 13:23:37.6499]
[*11/06/2019 13:23:37.6499] CAPWAP State: Configure
[*11/06/2019 13:23:37.6599] DOT11_CFG[0] Radio Mode is changed from Remote Bridge to Remote Bridge
.
..
.
[*11/06/2019 13:23:38.7799] DOT11_CFG[0]: Starting radio 0
[*11/06/2019 13:23:38.7799] DOT11_CFG[1]: Starting radio 1
[*11/06/2019 13:23:38.8899] EVENT-MeshRadioBackhaul[0]: BH_RATE_AUTO
[*11/06/2019 13:23:38.8899] EVENT-MeshSecurity: Intermodule message LSC_MODE_CHANGE
[*11/06/2019 13:23:38.9099] CAPWAP data tunnel UPDATE to forwarding SUCCEEDED
[*11/06/2019 13:23:38.9999] Setting Prefer-mode IPv4
[*11/06/2019 13:23:39.0499]
[*11/06/2019 13:23:39.0499]

CAPWAP State: Run

[*11/06/2019 13:23:39.0499] EVENT-MeshCapwap: CAPWAP joined controller
[*11/06/2019 13:23:39.0599] CAPWAP moved to RUN state stopping post join timer
[*11/06/2019 13:23:39.1599] CAPWAP data tunnel ADD to forwarding SUCCEEDED
[*11/06/2019 13:23:39.2299]

AP has joined controller ME

[*11/06/2019 13:23:39.2599]

Flexconnect Switching to Connected Mode

!
```

Dicas, truques e erros comuns

- Ao atualizar o MAP e o RAP para a mesma versão de imagem pelo fio, evitamos o download de imagens pelo ar (o que pode ser problemático em ambientes de RF "sujos").
- O aumento da largura do canal do link de backhaul de 5 GHz pode levar a uma menor SNR e a detecções de radares falsos (principalmente em 80 MHz e 160 MHz).
- A conectividade de link de malha não deve ser testada fazendo ping no MAP ou no RAP. Não será possível fazer ping neles quando o enlace de malha for ativado.
- É altamente recomendável testar a instalação em um ambiente controlado antes de

implantá-la no local.

- Se APs com antenas externas estiverem sendo usados, certifique-se de consultar o guia de implantação para verificar quais antenas são compatíveis e em que porta elas devem ser conectadas.
- Para fazer a ponte do tráfego de VLANs diferentes sobre o link de malha, o recurso VLAN Transparente precisa ser desabilitado.
- Considere ter um servidor syslog local para os APs, pois ele pode fornecer informações de depuração, caso contrário, só estará disponível com uma conexão de console.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.