Solucionar problemas e verificar a configuração inicial sem fio do SD-Access

Contents

Introduction

Este artigo descreve as etapas básicas de solução de problemas para identificar problemas básicos de conectividade nas configurações sem fio do Acesso SD. Ele descreverá os itens e comandos a serem verificados para isolar problemas na solução relacionados à rede sem fio.

Prerequisites

Requirements

Conhecimento da solução SD-Access

Uma topologia de acesso SD já configurada

Componentes Utilizados

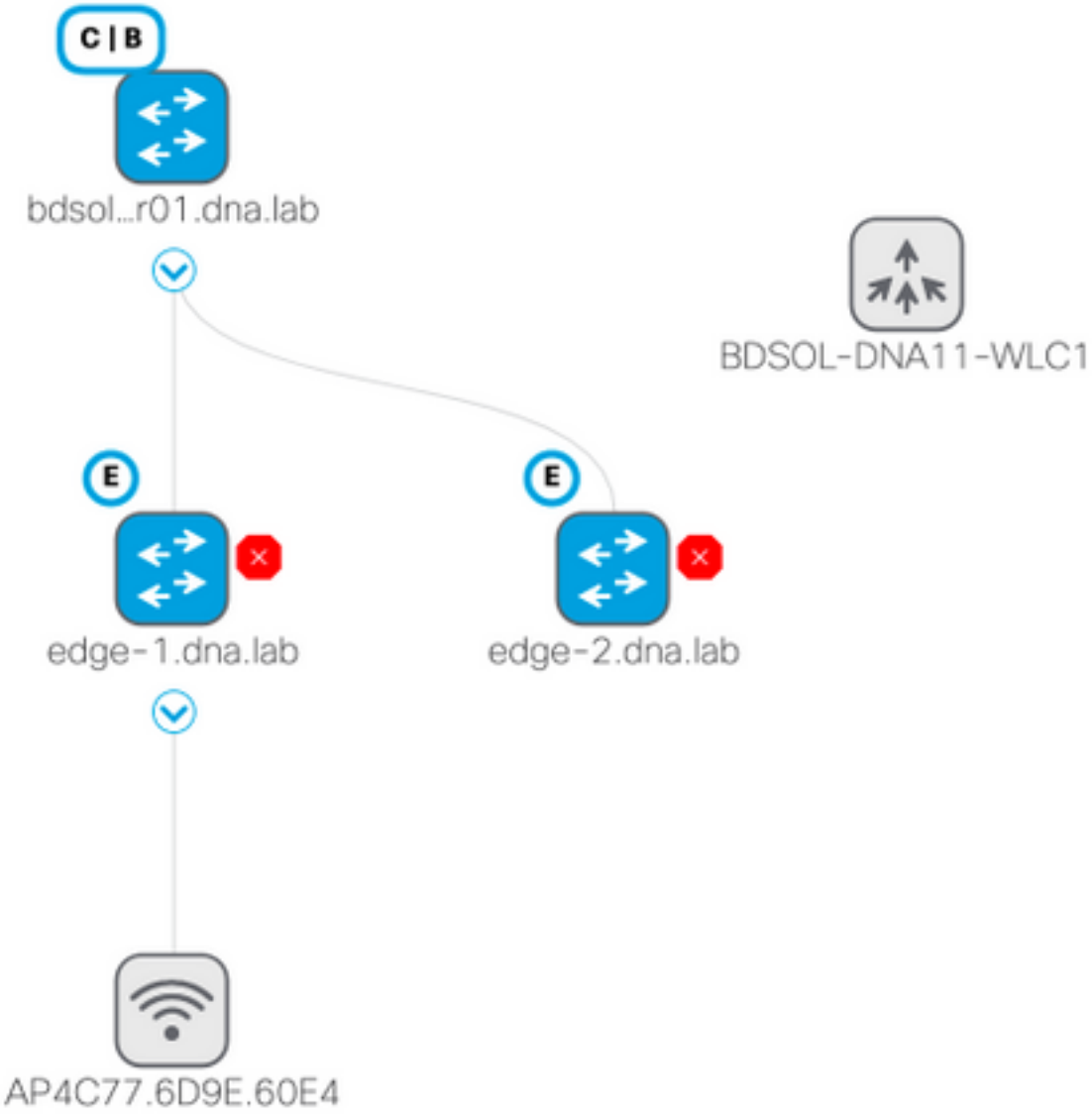
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando. Há outros tipos de dispositivos suportados para acesso SD sem fio, mas este artigo se concentra nos

dispositivos descritos nesta seção. Os comandos podem variar dependendo da plataforma e da versão do software.

8.5.151 Controlador sem fio

16.9.3 Switch 9300 como nó de borda

Topologia



Solucionar problemas e isolar

Verificações rápidas

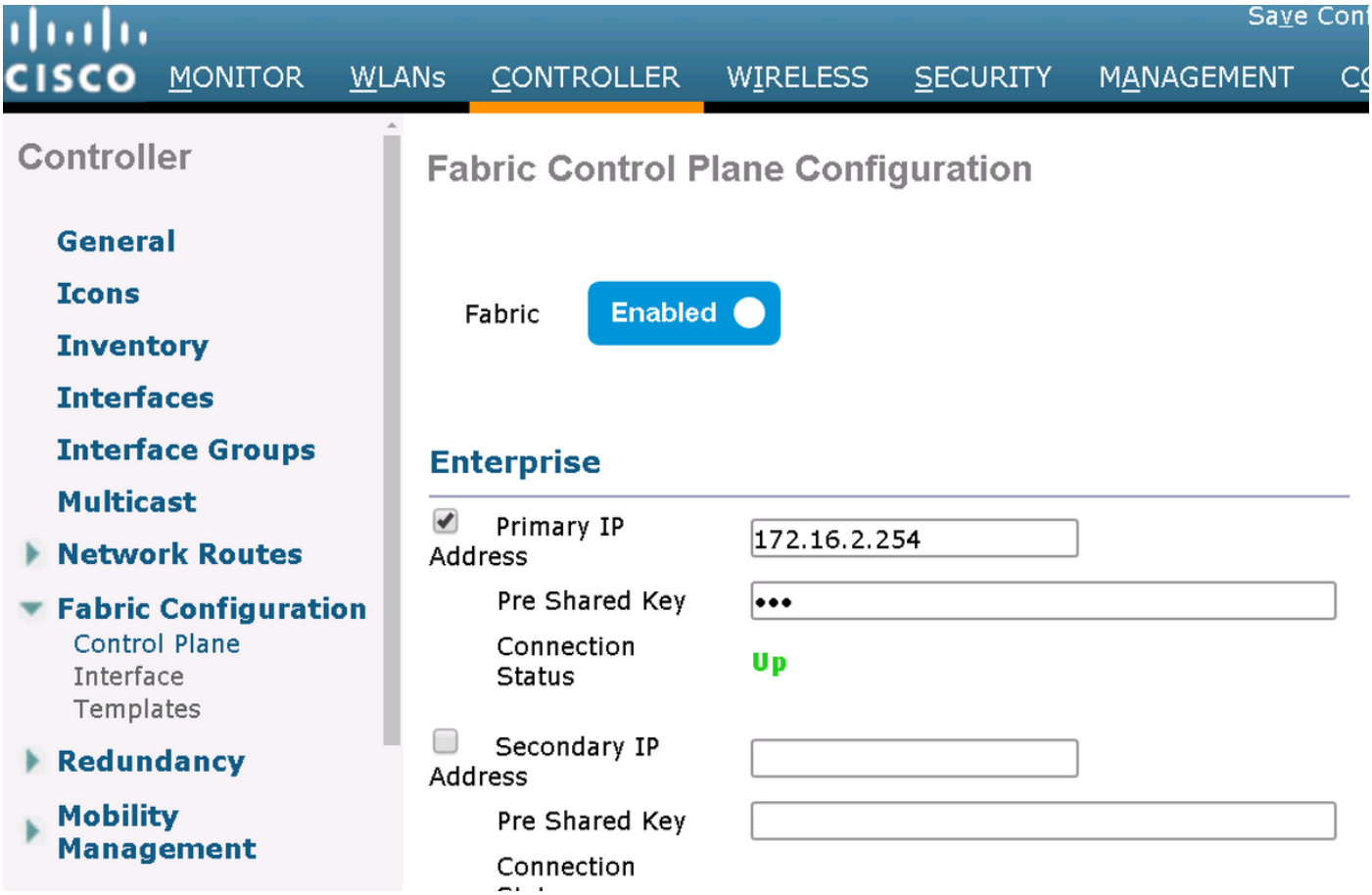
Há uma série de requisitos em cenários de acesso SD que geralmente são uma fonte de erros, portanto, verifique primeiro se esses requisitos foram atendidos:

- Certifique-se de que você tenha uma rota específica (e não esteja usando a padrão) apontando para a WLC no nó do plano de controle LISP

- Certifique-se de que seus APs estejam na Infra VN, usando a tabela de roteamento global
- Certifique-se de que os APs tenham conectividade com a WLC, fazendo ping na WLC a partir do próprio AP
- Certifique-se de que o status da estrutura do plano de controle na WLC esteja ativo
- Certifique-se de que os APs estejam no estado ativado para estrutura

cenário 1. Verificar o registro da WLC no plano de controle do servidor LISP/MAP

Quando você adiciona a WLC à malha no DNA Center, os comandos são enviados ao controlador para estabelecer uma conexão com o nó definido como plano de controle no DNA-C. A primeira etapa é garantir que esse registro seja bem-sucedido. Se a configuração LISP no plano de controle foi corrompida de alguma forma, esse registro pode falhar.



Se esse status for exibido como inativo, pode ser interessante executar depurações ou uma captura de pacotes entre a WLC e o plano de controle. O registro envolve TCP e UDP em 4342. Se o plano de controle não obteve a configuração adequada, ele pode responder com um TCP RST ao TCP SYN enviado pelo WLC.

O mesmo status pode ser verificado com **show fabric map-server summary** na linha de comando. O processo é depurado com **debug fabric lisp map-server all** na CLI da WLC. Para provocar uma tentativa de reconexão, você pode ir até o DNA Center e optar por remover a WLC da malha e adicioná-la novamente.

Possíveis motivos são linhas de configuração ausentes no plano de controle. Aqui está um exemplo de configuração de trabalho (somente a parte mais importante):

```
rtr-cp-mer-172_16_200_4#show run | s WLC
```

```
 locator-set WLC
  10.241.0.41
  exit-locator-set
 map-server session passive-open WLC
```

Se o ip da WLC estiver faltando (10.241.0.41 aqui) ou se o comando passive-open estiver faltando, o CP recusará a conexão da WLC.

As depurações a serem executadas são:

- '**debug capwap events enable**'
- '**debug capwap errors enable**'
- '**debug fabric ap-join events enable**'
- '**debug fabric ap-join detail enable**'
- '**debug fabric lisp map-server all enable**'

Aqui está um exemplo de um plano de controle que não atende a WLC

```
*msfMsgQueueTask: May 07 14:08:10.080: Sent map-request to MS 10.32.47.128 for AP 10.32.58.36
VNID 4097
*msfMsgQueueTask: May 07 14:08:10.080: No messages are present in the Client list for Local UDP
socket
*msfMsgQueueTask: May 07 14:08:10.080: msfSendLocalUDPSocketMessage:637 Message get for UDP file
socket list with path /tmp/msif_local_udp_socket_file failed
*osapiBsnTimer: May 07 14:08:15.179: Map-reply timer for MS IP 10.32.47.128 expired for AP IP
10.32.58.36 and VNID 4097
*msfMsgQueueTask: May 07 14:08:15.179: msfQueue: recieved LISP_MAP_SERVER_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: Added AP 10.32.58.36 VNID 4097 for long retry map-request
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: No messages are present in the Client list for Local UDP
socket
*msfMsgQueueTask: May 07 14:08:15.179: msfSendLocalUDPSocketMessage:637 Message get for UDP file
socket list with path /tmp/msif_local_udp_socket_file failed
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248
epoch 1525694896
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Response sent to 10.32.58.36:5248
*osapiBsnTimer: May 07 14:08:17.839: NAK Timer expiry callback
*msfMsgQueueTask: May 07 14:08:17.839: msfQueue: recieved LISP_MAP_SERVER_NAK_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:17.839: Started periodic NAK processing timer
*msfMsgQueueTask: May 07 14:08:17.839: Process list of AP (1) for which RLOC is not received
```

Aqui está um exemplo das depurações de WLC de um AP ingressando no estado desativado de estrutura porque o plano de controle de estrutura não tinha uma rota específica para a WLC

```
(POD3-WLC1) >*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:55:26.295: ip c0a82700,subnet ffffff00,l2vnid 8191,l3vnid 1001
*emWeb: Oct 16 08:55:26.295: Vnid Mapping added at index 2 with entries 192_168_39_0-
INFRA_VN,8191,4097,c0a82700,ffffff00.Count 3

*emWeb: Oct 16 08:55:26.295:
                              Log to TACACS server(if online): fabric vnid create name
192_168_39_0-INFRA_VN l2-vnid 8191 ip 192.168.39.0 subnet 255.255.255.0 l3-vnid 4097

*spamReceiveTask: Oct 16 08:55:26.295: Fabric is supported for AP f4:db:e6:61:24:a0 (Pod3-
AP4800). apType 54
```

```
*spamReceiveTask: Oct 16 08:55:26.295: spamProcessFabricVnidMappingAddRequest: Fabric Adding
vnid mapping for AP Pod3-AP4800 f4:db:e6:61:24:a0,lradIp 192.168.39.100,AP l2_vnid 0, AP l3_vnid
0
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name
192_168_39_0-INFRA_VN,l2vnid 8191,l3vnid 4097,ip c0a82700,mask ffffff00.Count 3

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP4800 f4:db:e6:61:24:a0,l3vnid 4097,PMS 192.168.30.55,SMS 0.0.0.0,mwarIp 192.168.31.59,lradIp
192.168.39.100
*emWeb: Oct 16 08:55:29.944:
                            Log to TACACS server(if online): save


(POD3-WLC1) >*spamApTask6: Oct 16 08:56:49.243: Fabric is supported for AP f4:db:e6:64:02:a0
(Pod3-AP3800). apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP3800 f4:db:e6:64:02:a0 can not be sent ,AP vnid mapping does not exist
```

Éinteressante observar que, se houver dois planos de controle em sua rede de estrutura, a WLC sempre procurará ambos para registro ou consultas. Espera-se que ambos os planos de controle forneçam respostas positivas nos registros, de modo que o WLC não registrará APs na estrutura se um dos dois planos de controle rejeitá-lo por qualquer motivo. Um plano de controle que não atende é aceitável, no entanto, e o plano de controle restante será usado.

Os APs alcançam a WLC através da tabela de roteamento global, mas o LISP ainda é usado para resolver a WLC. O tráfego enviado pelos APs para a WLC é o controle CAPWAP puro (sem vxlan envolvida), mas o tráfego de retorno enviado pela WLC para o AP será transportado por Vxlan na sobreposição. Você não poderá testar a conectividade da SVI do gateway AP na borda em direção à WLC porque, como é um gateway Anycast, o mesmo IP também existe no nó de borda. Para testar a conectividade, o melhor é fazer ping do próprio AP.

cenário 2. Os pontos de acesso não estão obtendo um endereço IP

Espera-se que os pontos de acesso obtenham um endereço IP do AP Poo, no Infra VNI definido no DNA Center. Se isso não acontecer, isso geralmente significa que a porta do switch onde o AP está conectado não se moveu para a vlan correta. O switch, ao detectar (por meio do CDP) um ponto de acesso sendo conectado, aplicará uma macro switchport que definirá a switchport na vlan definida pelo DNA-C para o pool de APs. Se a porta de switch problemática não estiver de fato configurada com a macro, você pode definir a configuração manualmente (para que o AP obtenha um ip, junte-se à WLC e provavelmente atualize seu código e possivelmente resolva qualquer bug de CDP) ou solucionar problemas do processo de conexão do CDP. Opcionalmente, você pode configurar a integração do host para definir estaticamente a porta no DNA-Center para hospedar um AP, de modo que ele seja provisionado com a configuração correta.

As macros Smartport não entram automaticamente se o switch não foi provisionado com pelo menos um AP, você pode verificar se a macro do AP foi provisionada com a vlan correta (em vez da vlan 1 padrão)

```
Pod3-Edge1#show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=2045
```

Os comandos que o Cisco DNA-C envia para definir isso são

```
macro auto execute CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT builtin CISCO_LWAP_AUTO_SMARTPORT
ACCESS_VLAN=2045
macro auto global processing
```

cenário 3. Os pontos de acesso não têm um túnel vxlan construído em direção ao nó Fabric Edge

Quando um AP se une à WLC, a WLC (se o AP for compatível com a estrutura) registrará o AP no plano de controle como um tipo especial de cliente. O plano de controle solicitará o nó de borda de estrutura onde o AP está conectado para criar um túnel vxlan em direção ao AP.

O AP usará apenas o encapsulamento vxlan para enviar tráfego de cliente (e somente para clientes no estado RUN), portanto, é normal não ver nenhuma informação vxlan no AP até que um cliente de estrutura se conecte.

No AP, o comando **show ip tunnel fabric** mostrará as informações do túnel vxlan depois que um cliente tiver se conectado.

```
AP4001.7A03.5736#show ip tunnel fabric
Fabric GWs Information:
Tunnel-Id           GW-IP            GW-MAC        Adj-Status Encap-Type Packet-In Bytes-In
Packet-Out Bytes-out
        1    172.16.2.253 00:00:0C:9F:F4:5E           Forward      VXLAN     39731  4209554
16345   2087073
AP4001.7A03.5736#
```

No nó Fabric Edge, o comando **show access-tunnel summary** mostrará os túneis vxlan construídos em direção aos pontos de acesso. Os túneis serão mostrados assim que o plano de controle ordenar sua criação quando o AP entrar.

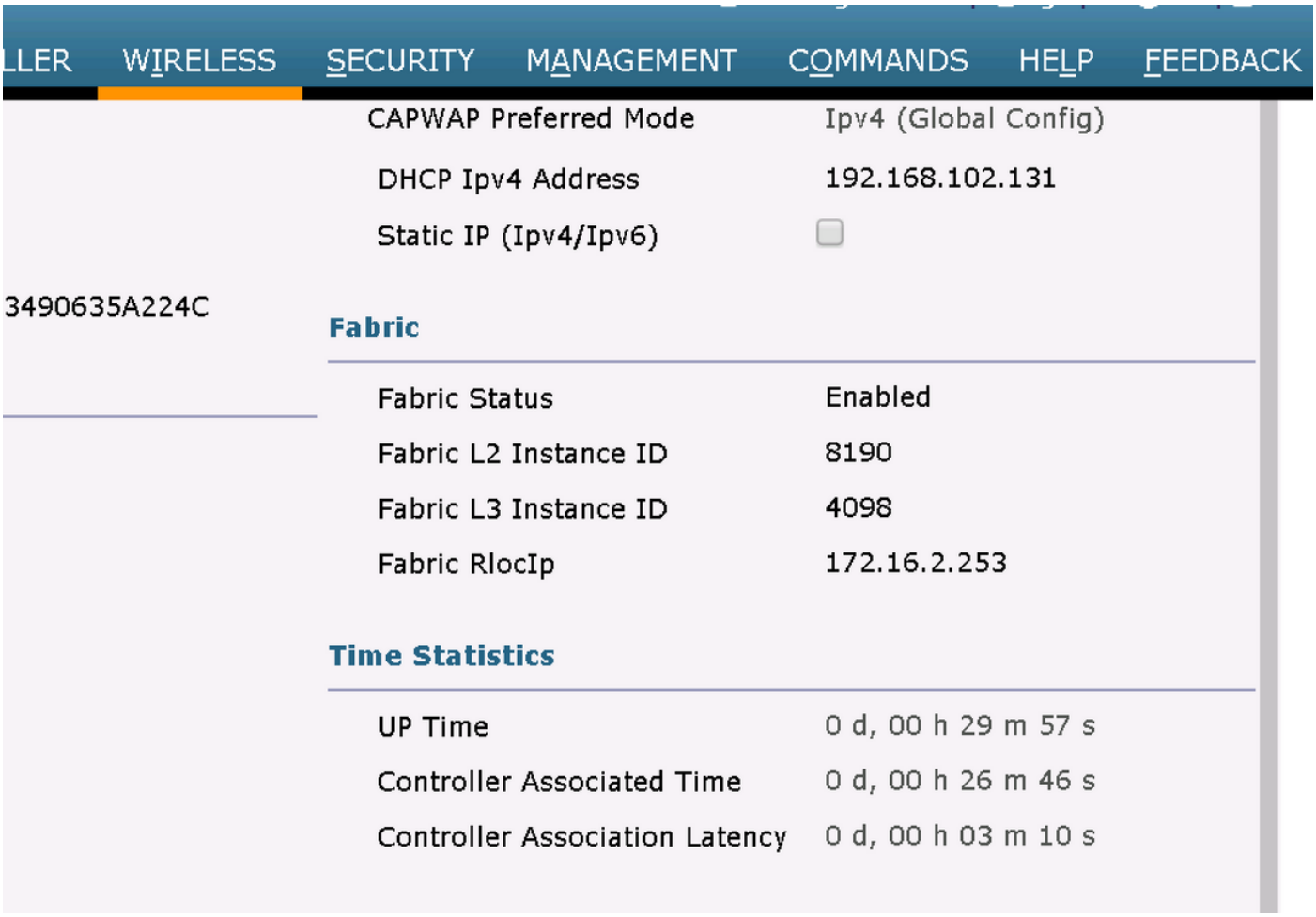
```
edge01#show access-tunnel summ

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2


Name   SrcIP           SrcPort DestIP          DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac1    172.16.2.253    N/A     192.168.102.130 4789    2
Ac0    172.16.2.253    N/A     192.168.102.131 4789    2


Name   IfId            Uptime
------ ---------- --------------------
Ac1    0x0000003B 1 days, 22:53:48
Ac0    0x0000003A 0 days, 22:47:06
```

Você pode verificar na WLC, na página do ponto de acesso, o ID da instância L2 LISP correspondente a esse AP e, em seguida, verificar as estatísticas dessa instância na Borda da estrutura onde ela está conectada.




```
SDA-D-6880-1#show lisp instance-id 8188 ethernet statistics
LISP EID Statistics for instance ID 8188 - last cleared: never
Control Packets:
  Map-Requests in/out:                      0/0
    Encapsulated Map-Requests in/out:       0/0
    RLOC-probe Map-Requests in/out:         0/0
    SMR-based Map-Requests in/out:          0/0
    Map-Requests expired on-queue/no-reply  0/0
    Map-Resolver Map-Requests forwarded:    0
    Map-Server Map-Requests forwarded:      0
  Map-Reply records in/out:                 0/0
    Authoritative records in/out:           0/0
    Non-authoritative records in/out:       0/0
    Negative records in/out:                0/0
    RLOC-probe records in/out:              0/0
    Map-Server Proxy-Reply records out:     0
  Map-Register records in/out:              24/0
    Map-Server AF disabled:                 0
    Authentication failures:                0
  Map-Notify records in/out:                0/0
    Authentication failures:                0
  Deferred packet transmission:             0/0
    DDT referral deferred/dropped:          0/0
    DDT request deferred/dropped:           0/0
```

cenário 4. entradas de túnel de acesso ausentes após um tempo

Épossível que os túneis de acesso sejam criados com êxito na primeira vez em que a WLC é provisionada através do Cisco DNA-C e adicionada à estrutura, mas ao reprovisionar a configuração sem fio (como a configuração da WLAN), observa-se que as entradas do túnel de acesso para APs estão ausentes, resultando na impossibilidade de os clientes sem fio obterem o IP com êxito.

A topologia é 9500(CP) —> 9300 (Edge) —> AP —> Wireless Client.

As entradas são observadas corretamente em **show access-tunnel summary** no nó de borda:

```
edge_2#show access-tunnel summary

Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1


Name SrcIP SrcPort DestIP DstPort VrfId
------ -------------- ------- -------------- ------- ----
Ac0 172.16.3.98 N/A 172.16.3.131 4789 0


Name IfId Uptime
------ ---------- --------------------
Ac0 0x0000003C 5 days, 18:19:37
```

Mas ao verificar **show platform software fed switch ative ifm interfaces access-tunnel,** a entrada para o AP está ausente ou falhou ao ser programada no hardware neste exemplo.

```
edge_2#show platform software fed switch active ifm interfaces access-tunnel
Interface IF_ID State
----------------------------------------------------------------
Ac0 0x0000003c FAILED
```

Para obter mais saídas:

```
edge_2#sh platform software access-tunnel switch active F0
Name SrcIp DstIp DstPort VrfId Iif_id Obj_id Status
-------------------------------------------------------------------------------------------
Ac0 98.3.16.172 131.3.16.172 0x12b5 0x000 0x00003c 0x00585f Done


edge_2#sh platform software access-tunnel switch active R0
Name SrcIp DstIp DstPort VrfId Iif_id
-----------------------------------------------------------------------
Ac0 172.16.3.98 172.16.3.131 0x12b5 0x0000 0x00003c
```

Você precisa comparar as diferentes saídas e cada túnel mostrado pelo **show access-tunnel summary** deve estar presente em cada uma delas.

cenário 5. clientes sem fio não conseguem obter um endereço IP

Se o túnel vxlan estiver presente e parecer bom, mas os clientes sem fio não conseguirem obter

sistematicamente um endereço IP, você talvez esteja enfrentando um problema da opção 82. Como o DHCP DISCOVER do cliente é encaminhado pelo gateway Anycast no nó de borda, haveria problemas para o servidor DHCP OFFER ser enviado ao nó de borda direita pela borda na volta. É por isso que a borda da estrutura que encaminha o DHCP DISCOVER acrescenta um campo de opção 82 ao DHCP DISCOVER que contém o RLOC da estrutura real (loopback ip) do nó de borda codificado junto com outras informações. Isso significa que o servidor DHCP deve suportar a opção 82.

Para solucionar problemas do processo DHCP, faça capturas nos nós da estrutura (especialmente no nó da borda do cliente) para verificar se a borda da estrutura está anexando o campo da opção 82.

cenário 6. A malha de convidado/autenticação da Web não está funcionando/não está redirecionando clientes

O cenário de estrutura para convidados é extremamente semelhante ao da Central Web Authentication (CWA) nos access points Flexconnect e funciona exatamente da mesma forma (mesmo que os APs de estrutura não estejam no modo flexconnect).

A ACL e a URL de redirecionamento devem ser retornadas pelo ISE no primeiro resultado de autenticação MAC. Verifique-os nos logs do ISE e na página de detalhes do cliente na WLC.

A ACL de redirecionamento deve estar presente como uma ACL Flex na WLC e deve conter instruções "permit" em relação ao endereço IP do ISE na porta 8443 (pelo menos).

O cliente deve estar no estado "CENTRAL_WEBAUTH_REQ" na página de detalhes do cliente na WLC. O cliente não poderá fazer ping neste gateway padrão e isso é esperado. Se você não for redirecionado, poderá tentar digitar manualmente um endereço IP no navegador da Web do cliente (para descartar o DNS, mas o nome de host do ISE terá que ser resolvido mesmo assim). Você deve ser capaz de inserir o IP do ISE na porta 8443 no navegador do cliente e ver a página do portal, pois esse fluxo não será redirecionado. Se isso não acontecer, você está enfrentando um problema de ACL ou um problema de roteamento. Colete capturas de pacotes ao longo do caminho para ver onde os pacotes HTTP são parados.

Entender

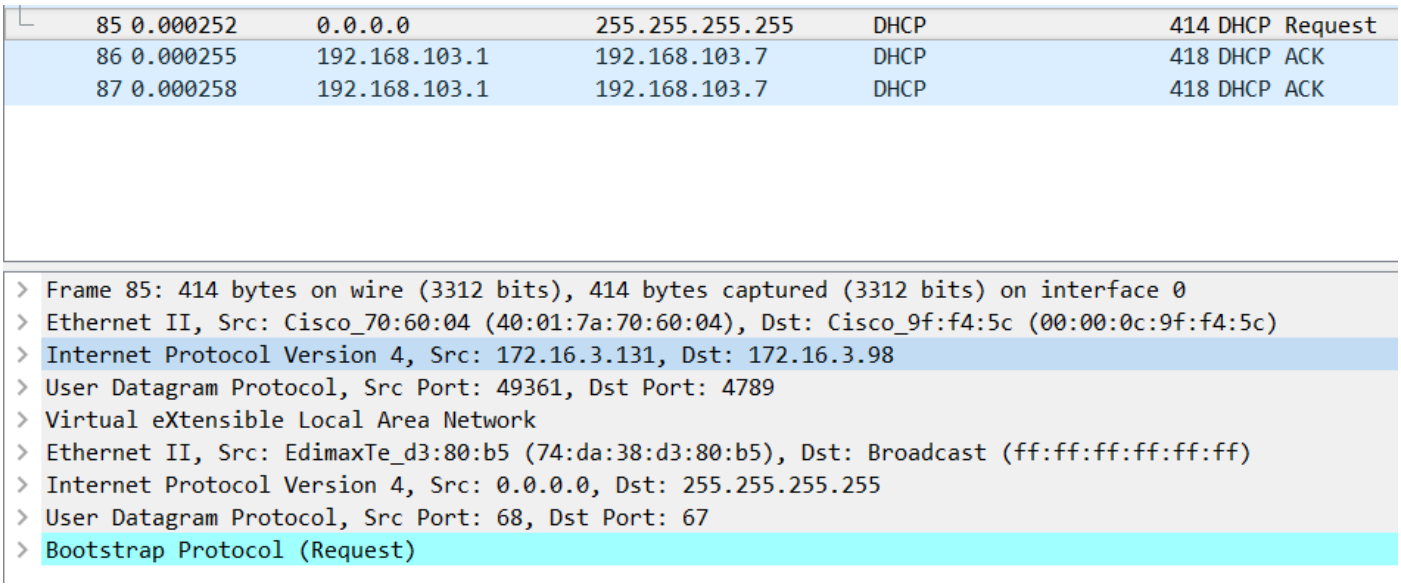
Como um cliente sem fio obtém um endereço IP na arquitetura de estrutura

65	0.000191	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
66	0.000194	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
80	0.000234	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
81	0.000238	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
82	0.000241	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
83	0.000245	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
84	0.000248	0.0.0.0	255.255.255.255	DHCP	440	DHCP Request - Transaction ID 0x5fd8da22
85	0.000252	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request - Transaction ID 0x5fd8da22
86	0.000255	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22
87	0.000258	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22

A captura de pacotes é feita entre o AP de estrutura e a borda da estrutura. Os pacotes são duplicados porque dois pacotes DHCP Discover foram enviados. O tráfego era apenas de entrada e capturado na borda da malha.

Há sempre dois pacotes DHCP. Um enviado pelo CAPWAP diretamente ao controlador para

mantê-lo atualizado. O outro enviado por VXLAN para o nó de controle. Quando o AP recebe, por exemplo, uma oferta DHCP com VXLAN pelo servidor DHCP, ele envia uma cópia para a controladora com CAPWAP.



Para ver para onde o pacote foi enviado, você precisa clicar nele no Wireshark. Aqui podemos ver que a origem é nosso AP 172.16.3.131 e o pacote foi enviado para a Borda de estrutura 172.16.3.98. A borda da malha a encaminhou ao nó de controle.

Entender o fluxo de redirecionamento da Web em um cenário de estrutura

A ACL de redirecionamento na WLC define qual tráfego é redirecionado/interceptado em instruções deny correspondentes (há um deny implícito no final). Esse tráfego a ser redirecionado será enviado para a WLC dentro do encapsulamento CAPWAP para a WLC redirecionar. Ao corresponder uma instrução de permissão, ele não redireciona esse tráfego e o deixa passar e encaminha na estrutura (o tráfego para o ISE entra nessa categoria).

Registros do AP que ingressa na WLC no estado ativado para estrutura

Assim que o ponto de acesso se registrar na WLC, o controlador registrará seus endereços IP e MAC no SDA Control Node (LISP Map Server).

O AP ingressa na WLC no modo ativado por estrutura somente se a WLC receber o pacote LISP RLOC. Esse pacote é enviado para garantir que o AP esteja conectado a uma Borda de Estrutura.

As depurações usadas no WLC para este exemplo são:

- **'debug capwap events enable'**
- **'debug capwap errors enable'**
- **'debug fabric ap-join events enable'**
- **'debug fabric ap-join detail enable'**
- **'debug fabric lisp map-server all enable'**

Para o teste, o AP é reinicializado:

```
*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated
Payload 3 sent to 172.16.3.131:5256
```

*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: Cleaned up AP RLOC NAK entry for AP 172.16.3.131 vnid 4097 for BOTH MS
*msfMsgQueueTask: May 07 13:00:18.804: Inserted entry for AP IP 172.16.3.131 and VNID 4097, db idx 12
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply timer started for AP IP 172.16.3.131 and VNiD 4097
*msfMsgQueueTask: May 07 13:00:18.804: Creating new timer for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply Timer Started Successfully for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Not able to find nonce 0x3cd13556-0x81864b7b avl entry
*msfMsgQueueTask: May 07 13:00:18.804: FAIL: not able to find avl entry
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b inserted into nonce aVL tree for AP IP 172.16.3.131 VNID 4097 for MS 172.16.3.254
*msfMsgQueueTask: May 07 13:00:18.804: Set nonce 0x3cd13556-0x81864b7b for AP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b is updated for AP IP 172.16.3.131, VNID 4097 and MS IP 172.16.3.254, db idx 12
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and VNID 4097 to MS IP 172.16.3.254
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build allocating nonce
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmNeighbourCtrl payload sent to 172.16.3.131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for CcxRmMeas payload sent to 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS 172.16.3.254**
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP ext-logging AP ext-logging message sent to 172.16.3.131:5256
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to 172.16.3.131:5256
***msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS 172.16.3.254 is sent**
***msfMsgQueueTask: May 07 13:00:18.804: Sent map-request to MS 172.16.3.254 for AP 172.16.3.131 VNID 4097**
*msfMsgQueueTask: May 07 13:00:18.804: Invalid secondary MS IP 0.0.0.0 for map-request for AP IP 172.16.3.131
*msfMsgQueueTask: May 07 13:00:18.804: No messages are present in the Client list for Local UDP socket
*msfTcpTask: May 07 13:00:18.807: Sending the UDP control packet to queue task
*msfMsgQueueTask: May 07 13:00:18.807: msfQueue: recieved LISP_MAP_SERVER_UDP_PACKET_QUEUE_MSG
*msfMsgQueueTask: May 07 13:00:18.807: Mapping Record has locators and actions
*msfMsgQueueTask: May 07 13:00:18.807: Mapping record address 172.16.3.98 EID address 172.16.3.98
*msfMsgQueueTask: May 07 13:00:18.807: Got AVL entry for nonce 0x3cd13556-0x81864b7b in map-reply for AP IP 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and VNID 4097 in map-reply to spam task**
***msfMsgQueueTask: May 07 13:00:18.807: Added RLOC 172.16.3.98 for AP IP 172.16.3.131**
***spamReceiveTask: May 07 13:00:18.807: Recieved Fabric rloc response from msip 172.16.3.254 with apvnid 4097,fabricRLoc 172.16.3.98 apip 172.16.3.131 apRadMac 70:70:8b:20:29:00**

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.