#CiscoLive

The bridge to possible

Troubleshooting DHCP in SDA Fabric

Mohitkumar Savaliya - Technical Consulting Engineer
Alejandro Jon Torres – Technical Leader

TSCENT-2021

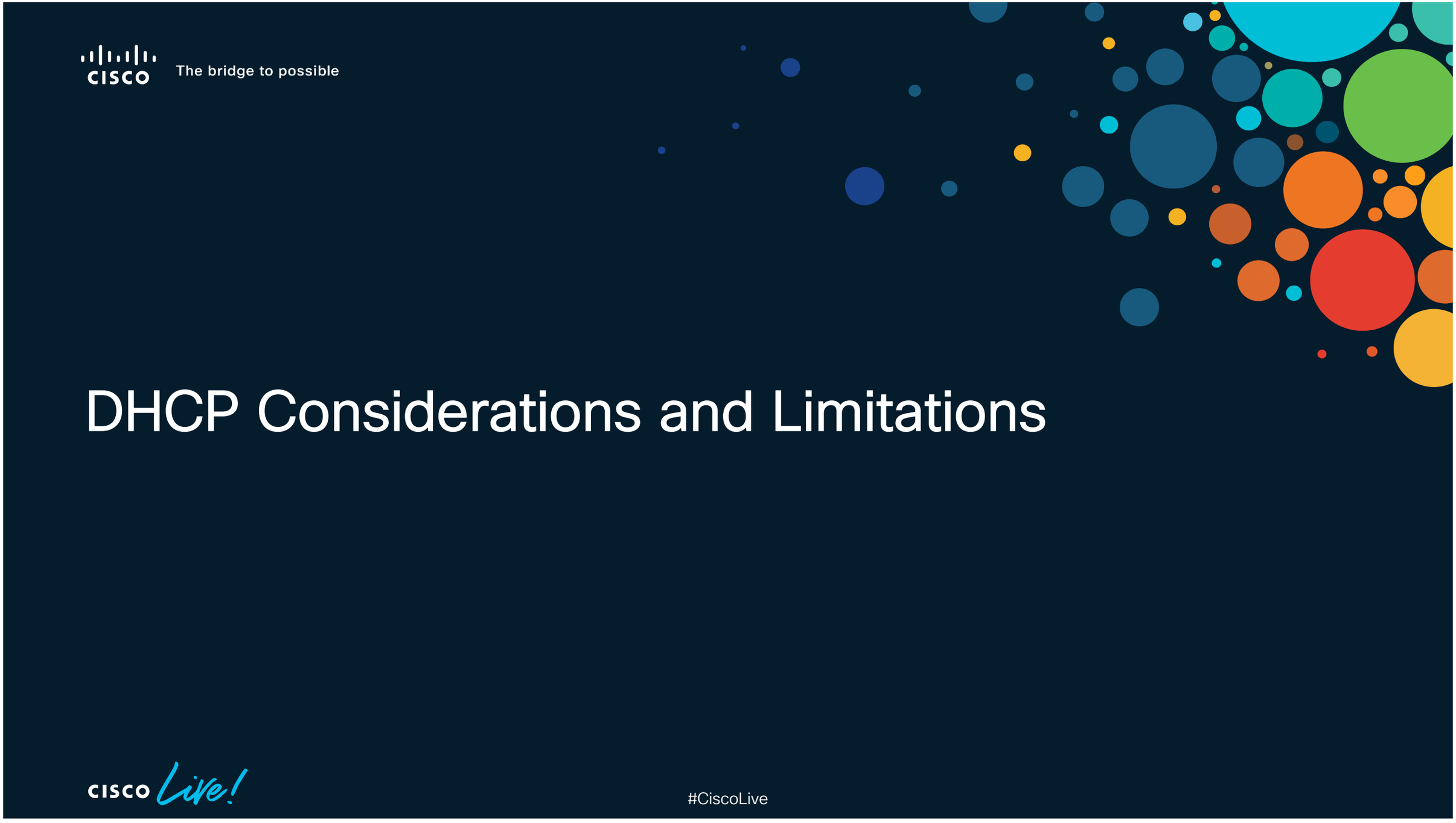
Cisco Live!

Agenda

- DHCP Considerations and Limitations
- Life of a DHCP Packet in the Fabric
- DHCP in Fabric Enabled Wireless
- PXE Boot Considerations and Limitations

Introduction

- This presentation will cover identifying and troubleshooting common DHCP issues seen in SDA Fabrics



DHCP Considerations and Limitations

DHCP Considerations and Limitations

- **DHCP Servers cannot be connected to a Fabric Edge as part of a Fabric IP Pool**

  Any DHCP packet received with VXLAN encapsulation that is destined to anything except the Anycast gateway IP address will be dropped (*this does not apply for L2 Only Pools*)

- **DHCP Servers must accept and preserve DHCP Option 82**

  DHCP Relay Agents will use as source IP the Anycast IP of the incoming SVI when relaying the packet. As such, additional information is required to identify the correct Edge/Relay Agent when Offer/Ack comes back.

- **Avoid disabling DHCP snooping as a workaround when troubleshooting**

  DHCP snooping is the component responsible with inserting Option 82 in the Discover payload, and without this value offers will not be forwarded to the appropriate Fabric Edge.

DHCP Considerations and Limitations - continuation

- **Bi-directional applications might not work with relays (IP helper-address)**

  IP Helper addresses can relay a variety of UDP protocols which are by default forwarded or configured to be forwarded ("ip forward-protocol udp"), but only DHCP includes a value like Option 82 to identify the origin of the packet.

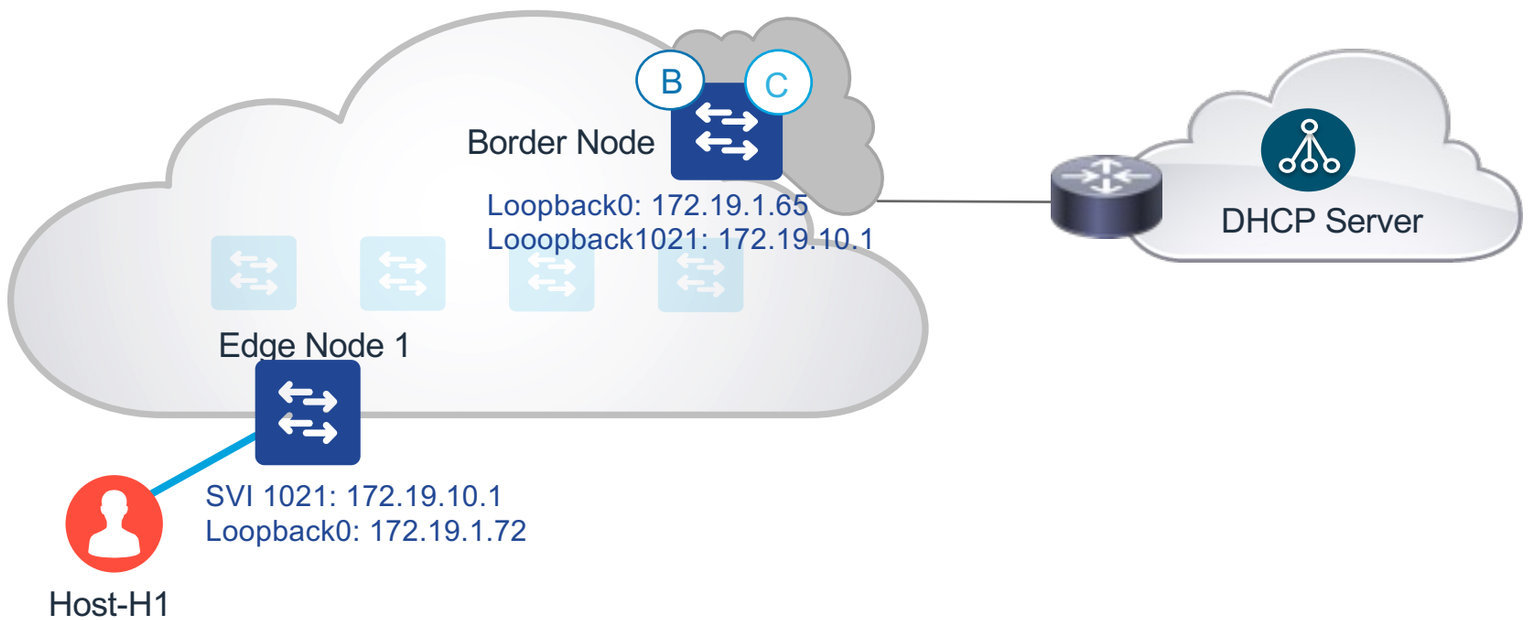
- **The following UDP port combinations are allowed combinations for DHCP packet processing/relaying:**

  Source Port: 68 Destination Port: 67
  Source Port: 67 Destination Port: 67
  Source Port: 67 Destination Port: 68

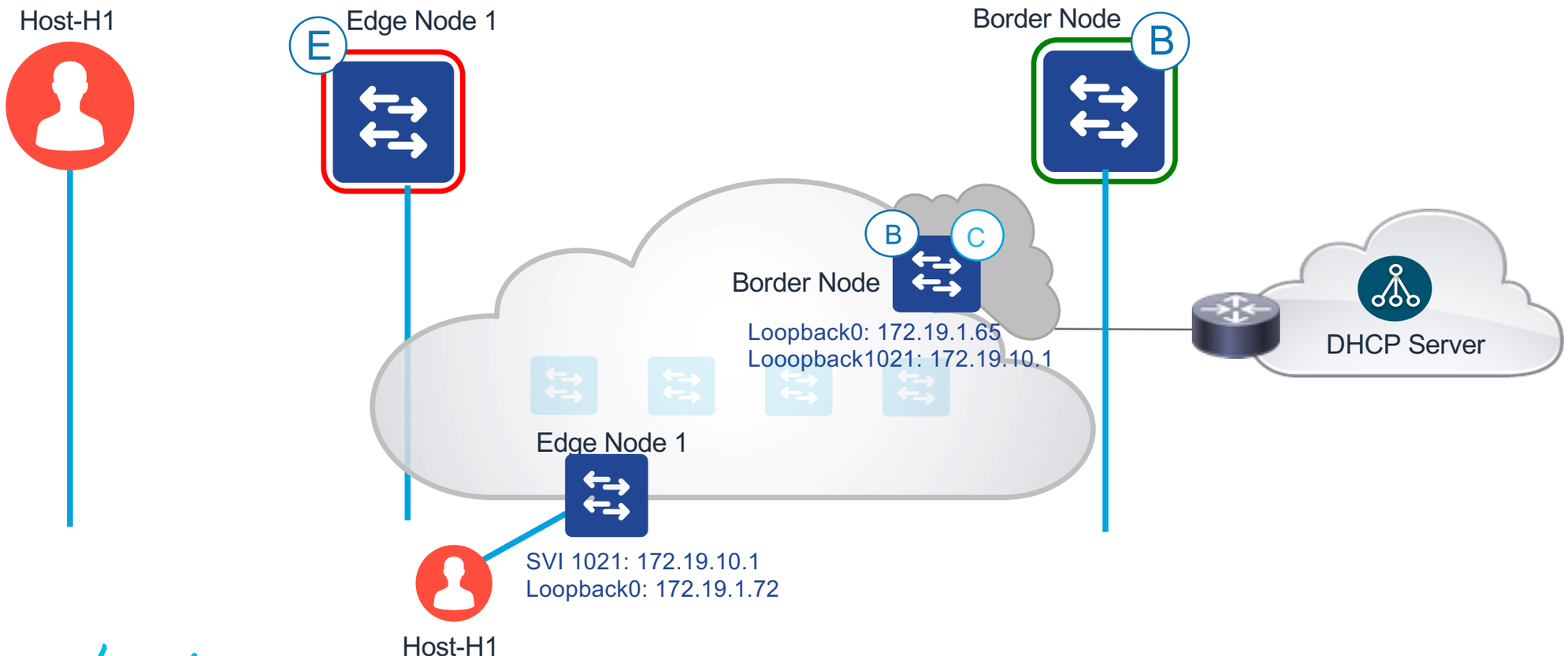
The bridge to possible

Life of a DHCP Packet in the Fabric

Life of a DHCP Packet [Discover]



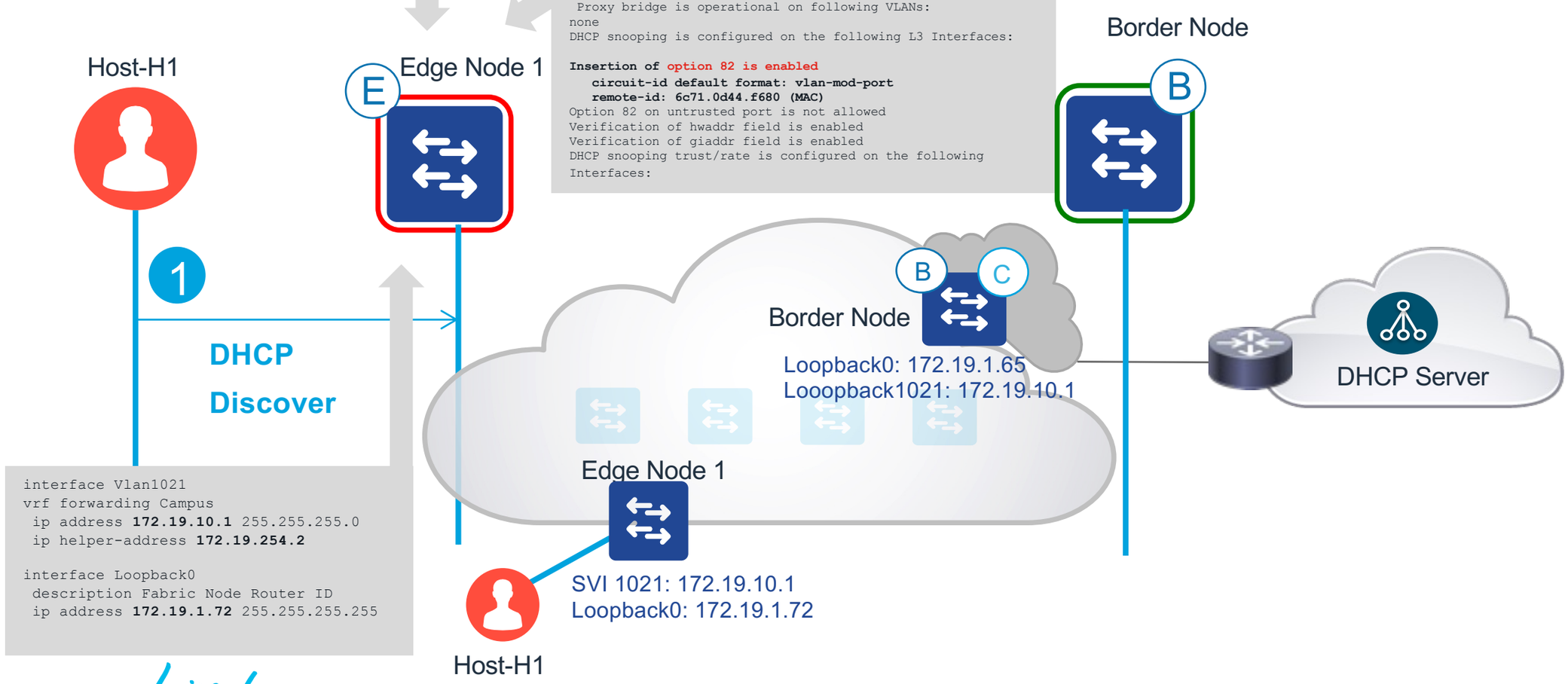
Life of a DHCP Packet [Discover]



Life of a DHCP Packet [Discover]

```
Edge1#show mac address interface te1/0/4
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1021    d4e8.801f.4876    DYNAMIC     Te1/0/4
```

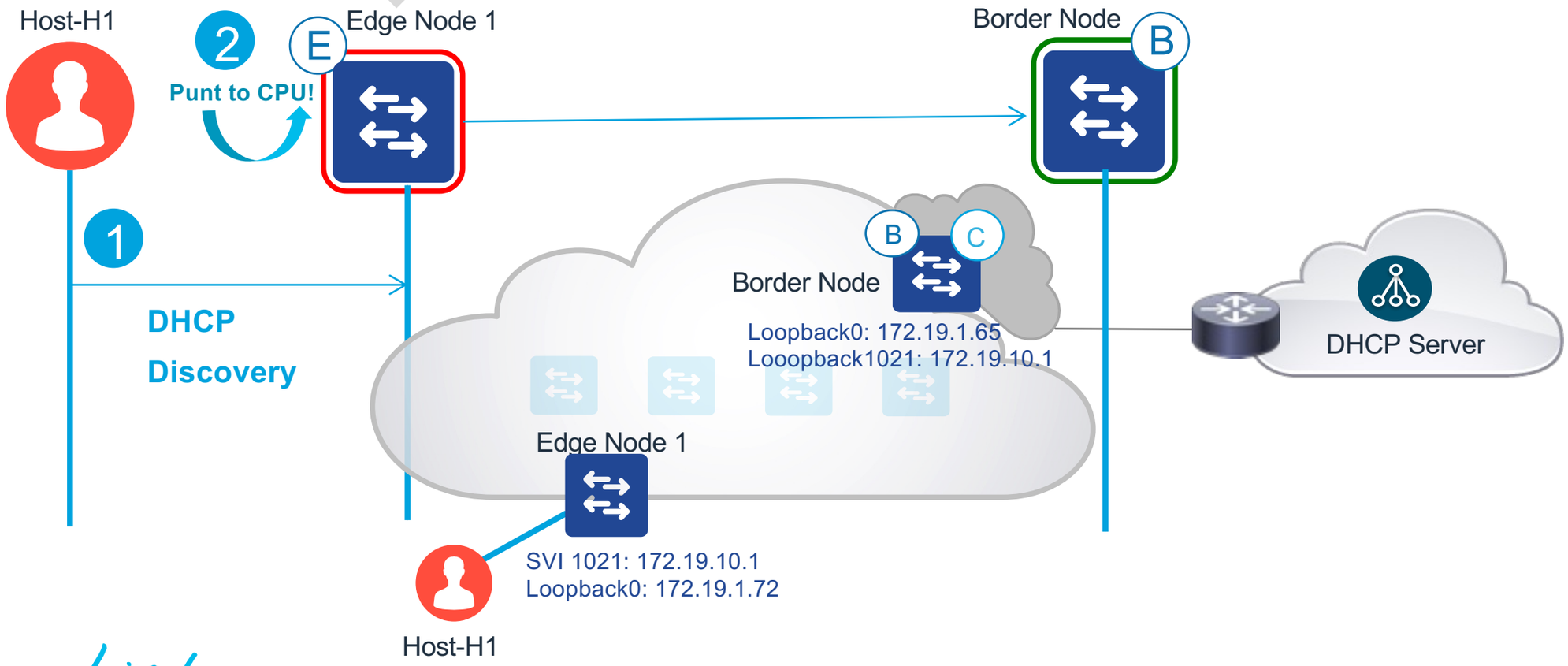
```
Edge1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1021,1023-1025,1028-1029,1031,1033,1035,1039,1041,1044,2045-
2047
DHCP snooping is operational on following VLANs:
1021,1023-1025,1028-1029,1031,1033,1035,1039,1041,1044,2045-
2047
 Proxy bridge is configured on following VLANs:
none
 Proxy bridge is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 6c71.0d44.f680 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following
Interfaces:
```




```
interface Vlan1021
vrf forwarding Campus
 ip address 172.19.10.1 255.255.255.0
 ip helper-address 172.19.254.2

interface Loopback0
 description Fabric Node Router ID
 ip address 172.19.1.72 255.255.255.255
```

Life of a DHCP Packet [Discover]

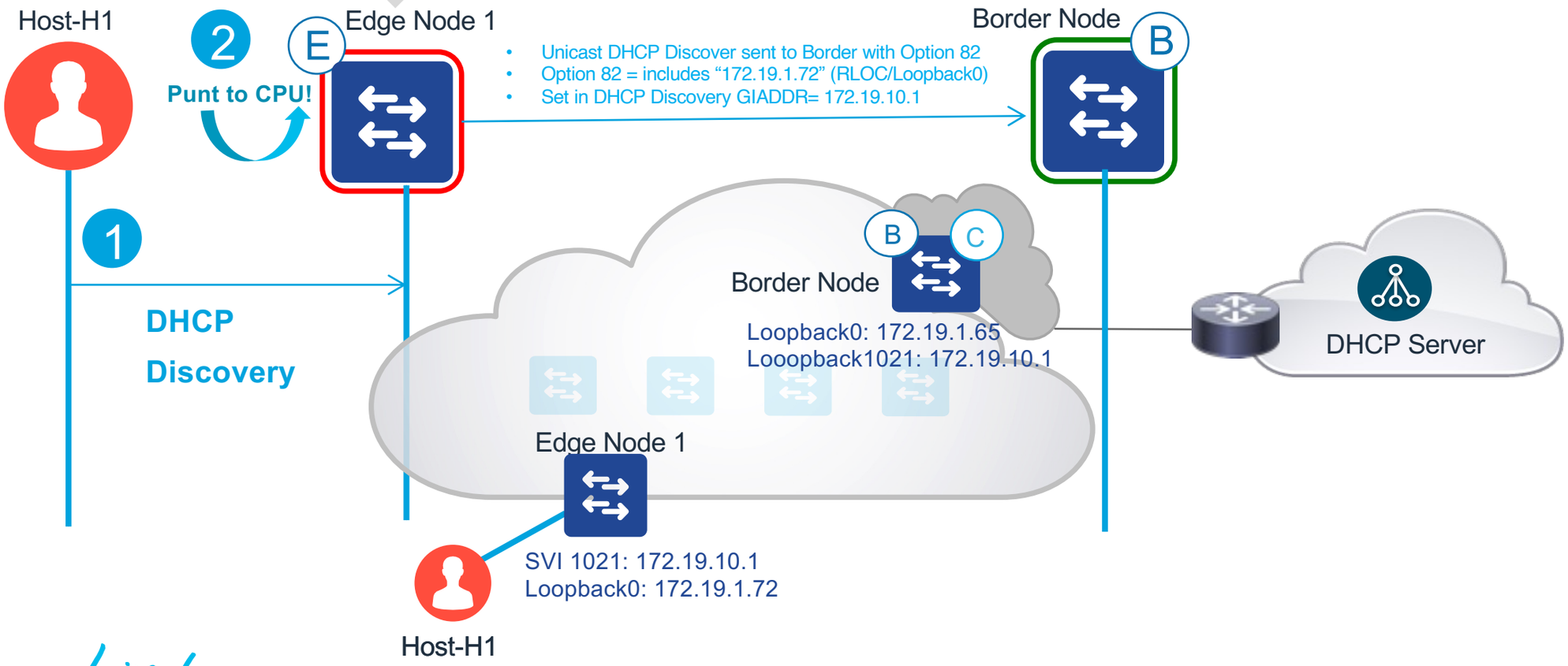
```
#debug ip dhcp snooping packets
#debug ip dchp snooping events
009388: *Apr 21 03:21:24.322: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Te1/0/4, MAC da: ffff.ffff.ffff, MAC sa:
d4e8.801f.4876, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr:
d4e8.801f.4876, efp_id: 0, vlan_id: 1021, bootpflag:0x32768(Broadcast)
009389: *Apr 21 03:21:24.322: DHCP_SNOOPING: add relay information option.
009390: *Apr 21 03:21:24.322: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
009391: *Apr 21 03:21:24.322: :VLAN case : VLAN ID 1021
009392: *Apr 21 03:21:24.322:  VRF id is valid
009393: *Apr 21 03:21:24.322: LISP ID is valid, encoding RID in srloc format
009395: *Apr 21 03:21:24.322: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (1021)
009396: *Apr 21 03:21:24.322: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan1021.
```



Life of a DHCP Packet [Discover]

```
** EPC CPU CAPTURE, Relayed DHCP Discover**

Edge1#show monitor capture cap buffer display-filter bootp.type==1 detail | se Agent Information
    Option: (82) Agent Information Option
        Length: 20
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 6
            Agent Circuit ID: 000403fd0104
        Option 82 Suboption: (2) Agent Remote ID
            Length: 10
            Agent Remote ID: 030800100301ac130148  == 172.19.1.72!!
```

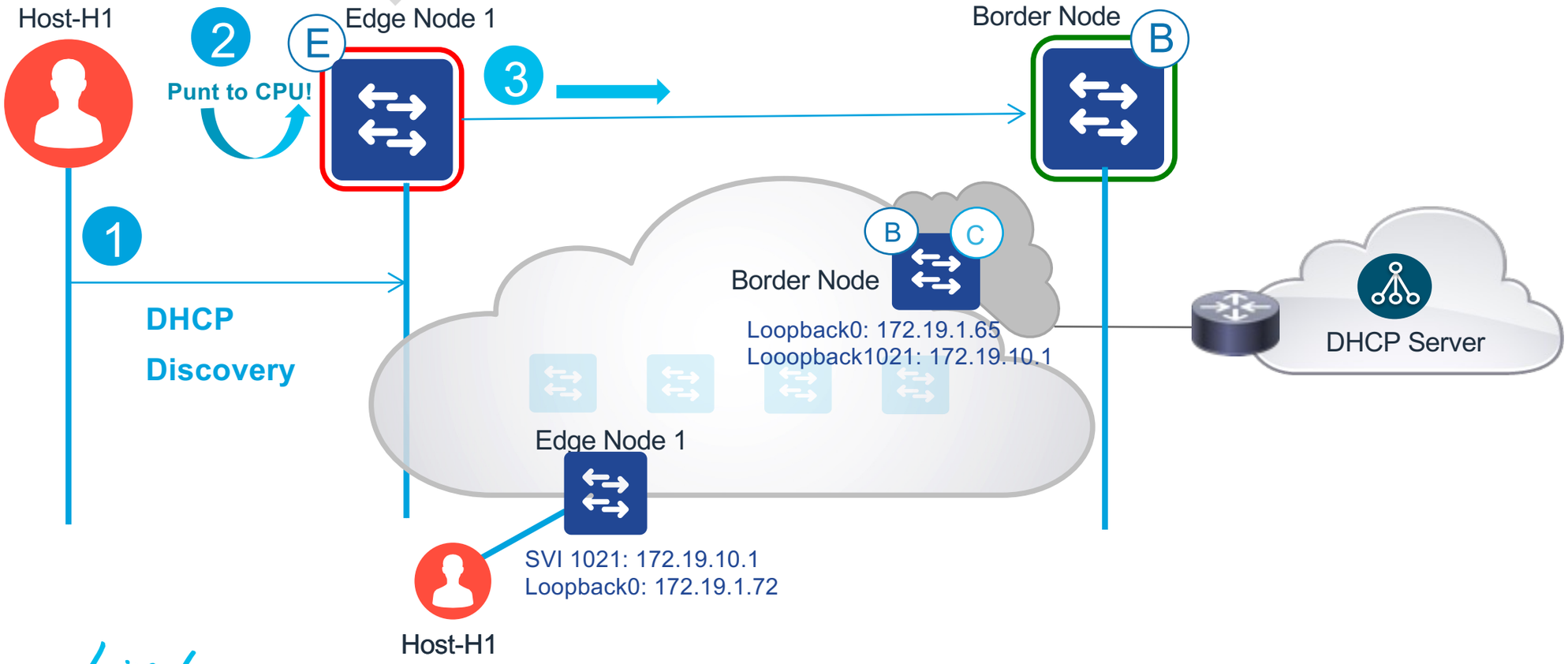
```
** EPC CPU CAPTURE, Both DHCP Discovers**

Edge1#show monitor capture cap buffer display-fiter bootp.type==1 detail | i Relay
    Relay agent IP address: 0.0.0.0    ------ Original, punted DHCP discover
    Relay agent IP address: 172.19.10.1  ---- Injected DHCP Discover relay
```



Life of a DHCP Packet [Discover]

```
Edge1#show ip cef vrf Campus 172.19.254.2
172.19.252.0/22
  nexthop 172.19.1.65 LISP0.4099
Edge1#show ip cef 172.19.1.65
172.19.1.65/32
  nexthop 172.19.1.70 TenGigabitEthernet1/0/3
```

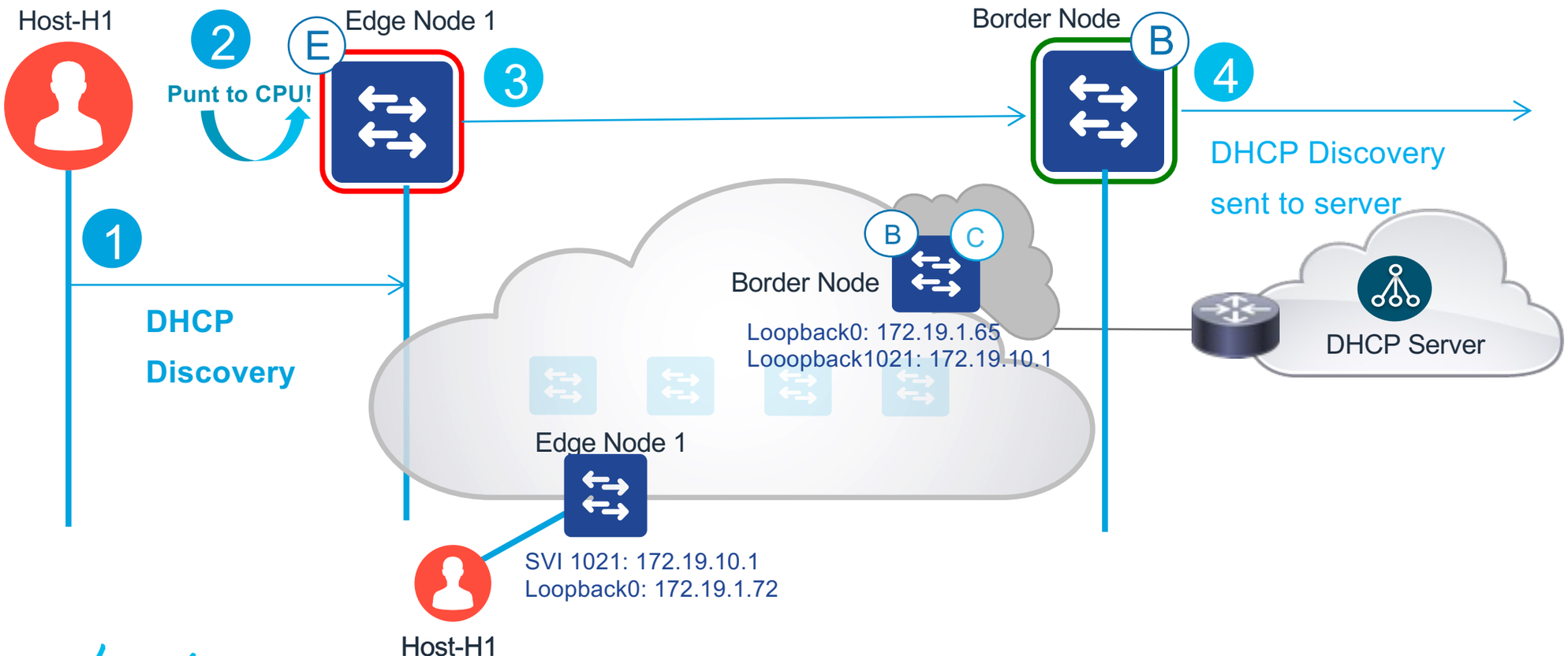
- Traffic is sent to DHCP server from 172.19.10.1 (SVI) to 172.19.254.2 (Server)
- Troubleshooting steps on Fabric Edge:
  - What is the CEF forwarding decision to reach the DHCP server?
  - Is the route to the Border RLOC known as /32?



Life of a DHCP Packet [Discover]

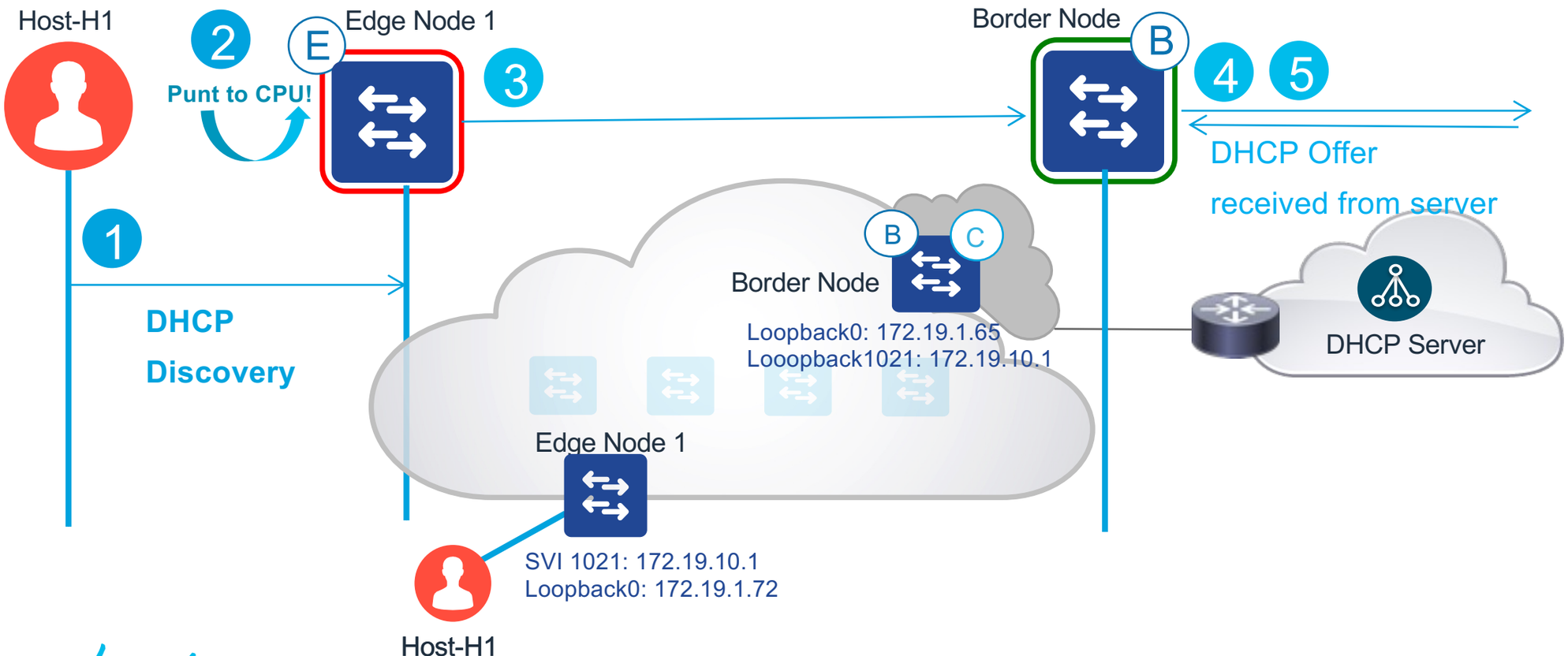
- Troubleshooting steps on Border Nodes and Fusion Devices:
  - Does the Border have a route to the DHCP server?
  - Is route leaking working in Fusion Devices such that Borders can reach the DHCP subnet?
  - Use extended ping - “ping vrf Campus 172.19.254.2 source Loopback1021” to check

  NOTE: If multiple Borders exist, it is expected for only one of them to be able to ping (as Anycast Gateway Loopbacks are used across borders, only one of them will receive the reply)
  - Was Option 82 inserted in the DHCP Discover? - Packet Capture



Life of a DHCP Packet [Offer]

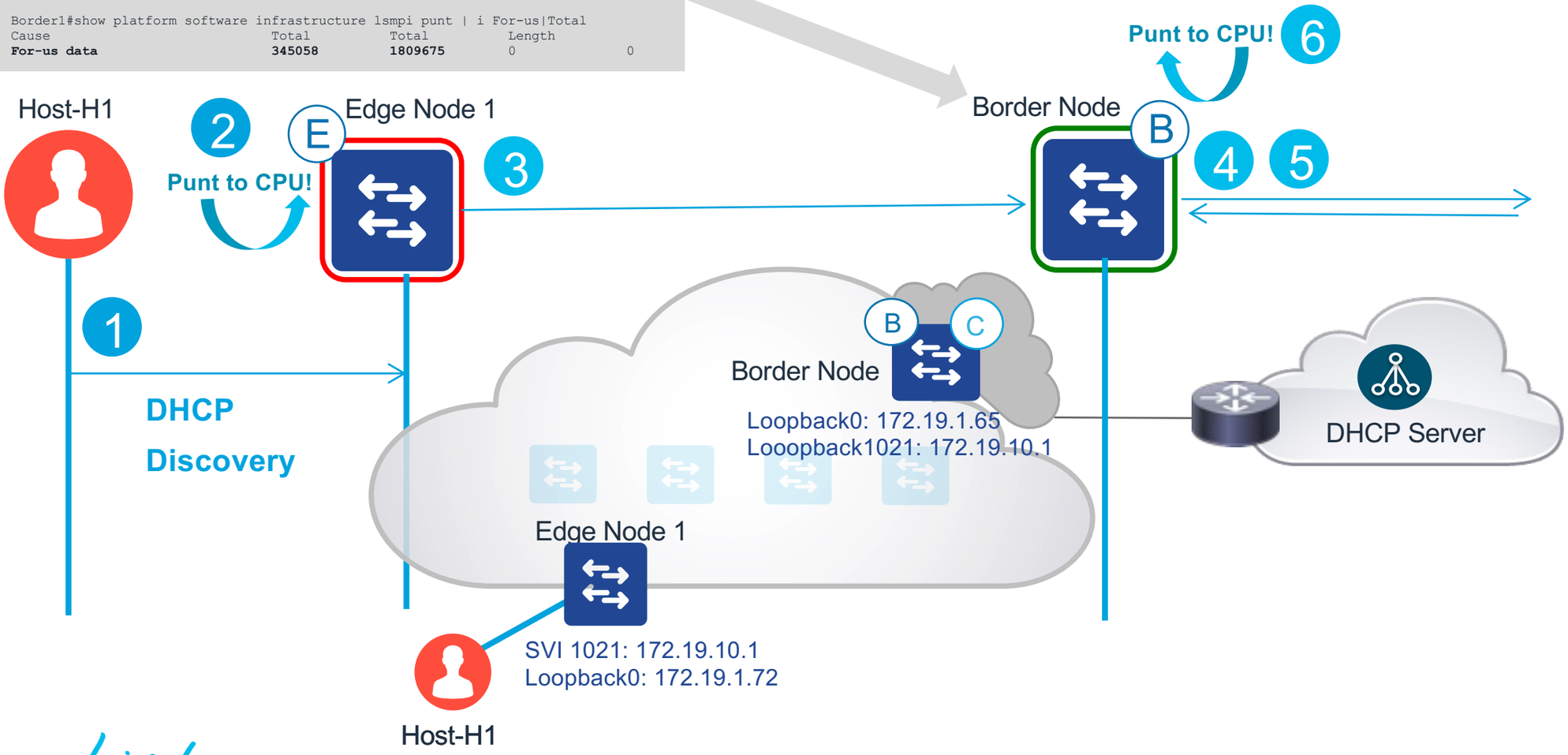
- DHCP address pool selected using GIADDR= 172.19.10.1
- DHCP offer sent to GIADDR= 172.19.10.1 (DST IP)
- Option82 is copied into the Offer message
- Troubleshooting steps:
  - Is the DHCP Offer seen at the Border uplink? – Packet Capture
  - Is Option 82 present in the DHCP Offer? – Packet Capture



Life of a DHCP Packet [Offer]

```
** Borders have no DHCP snooping except by FIABs/L2 Handoffs**

Border1#show ip dhcp snooping
Switch DHCP snooping is disabled

Border1#show ip cef vrf Campus 172.19.10.1
172.19.10.1/32
  receive for Loopback1021

Border1#show platform software infrastructure lsmpi punt | i For-us|Total
Cause                           Total          Total          Length
For-us data                     345058         1809675        0              0
```

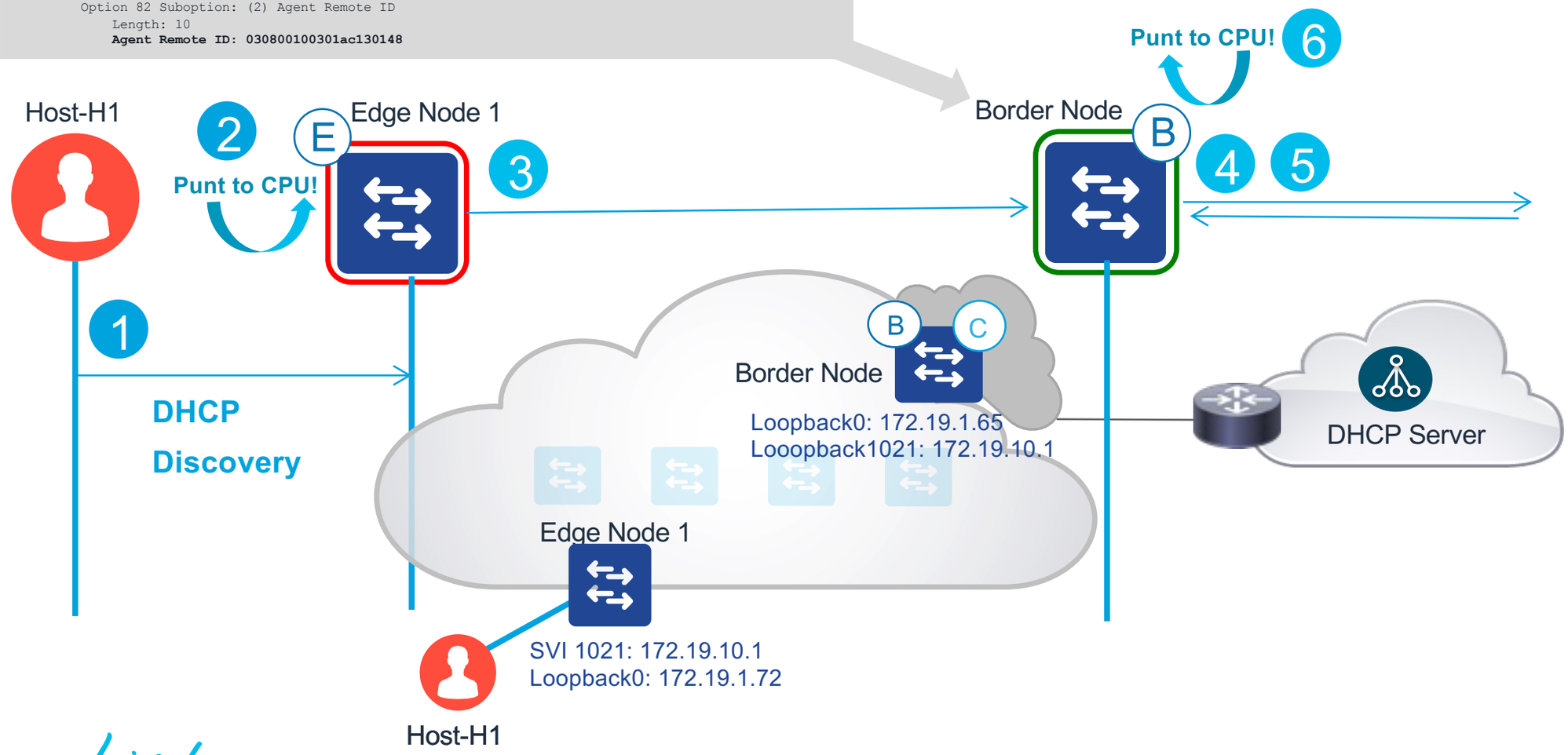
- DHCP Offer is processed in CPU path



Life of a DHCP Packet [Offer]

```
** EPC CPU Capture**

Border1#show monitor capture capture buffer displayu-filter bootp.type==2 detail | se Agent Infor
    Option: (82) Agent Information Option
        Length: 20
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 6
            Agent Circuit ID: 000403fd0104
        Option 82 Suboption: (2) Agent Remote ID
            Length: 10
            Agent Remote ID: 030800100301ac130148
```

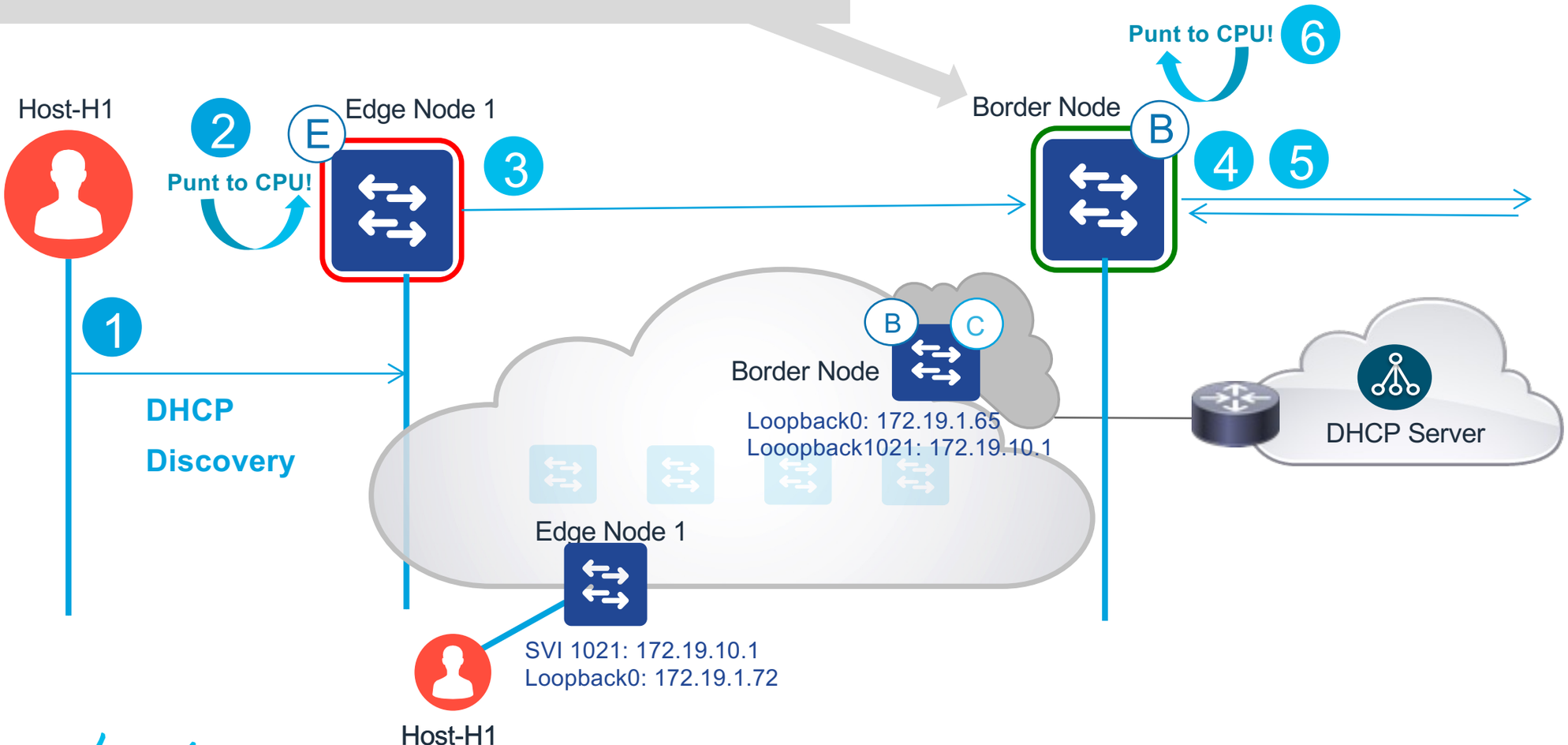
- Original Source RLOC can be extracted from DHCP Option82



Life of a DHCP Packet [Offer]

```
#debug platform software infrastructure punt

Border1#show log | i 172.19.254.2
*Apr 21 04:01:41.167:  Punt: IP proto UDP dst 67, src 67 (0x2) src 172.19.254.2, dst 172.19.10.1, from
table 2, intf Vl3045, encap ARPA, size 385, cause For-us data(L3)

*Apr 21 04:01:41.167: DHCP_SNOOP: <<< Glean pkt handler: dhcp packet is for lisp: encapsulate and
inject back dhcp-response packet
```

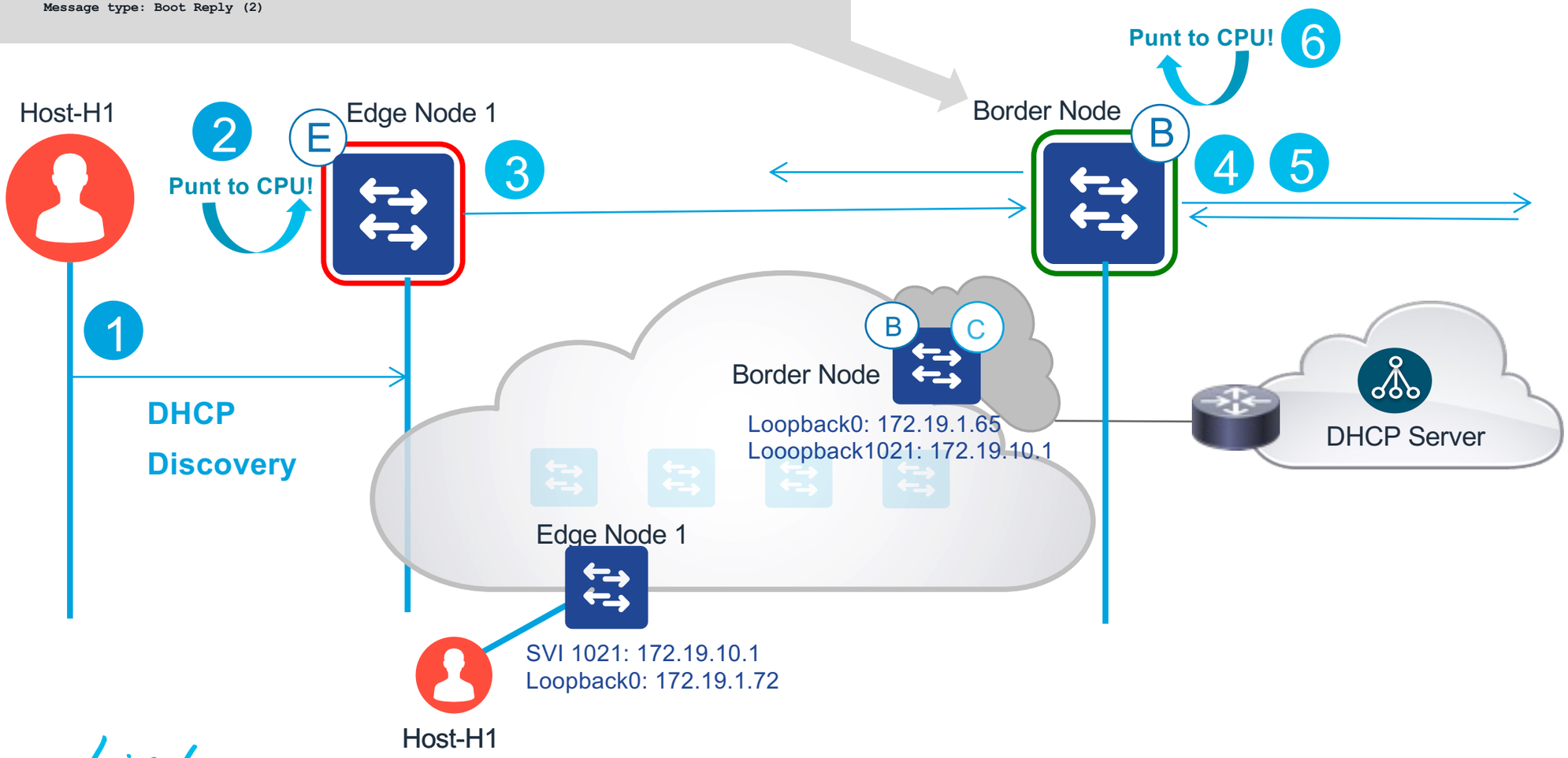
- Traffic is Punted as “For-Us”, then handed to DHCP Snooping process



Life of a DHCP Packet [Offer]

```
# EPC CPU Capture in Border (Injected Packet) -truncated-

Border1#show monitor capture cap buffer display-filter bootp.type==2 detail | se VXLAN Network|Internet
Internet Protocol Version 4, Src: 172.19.1.65, Dst: 172.19.1.72
    Flags: 0x0848, Don't Learn, VXLAN Network ID (VNI), Policy Applied
    VXLAN Network Identifier (VNI): 4099
Internet Protocol Version 4, Src: 172.19.254.2, Dst: 172.19.10.1
Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
```

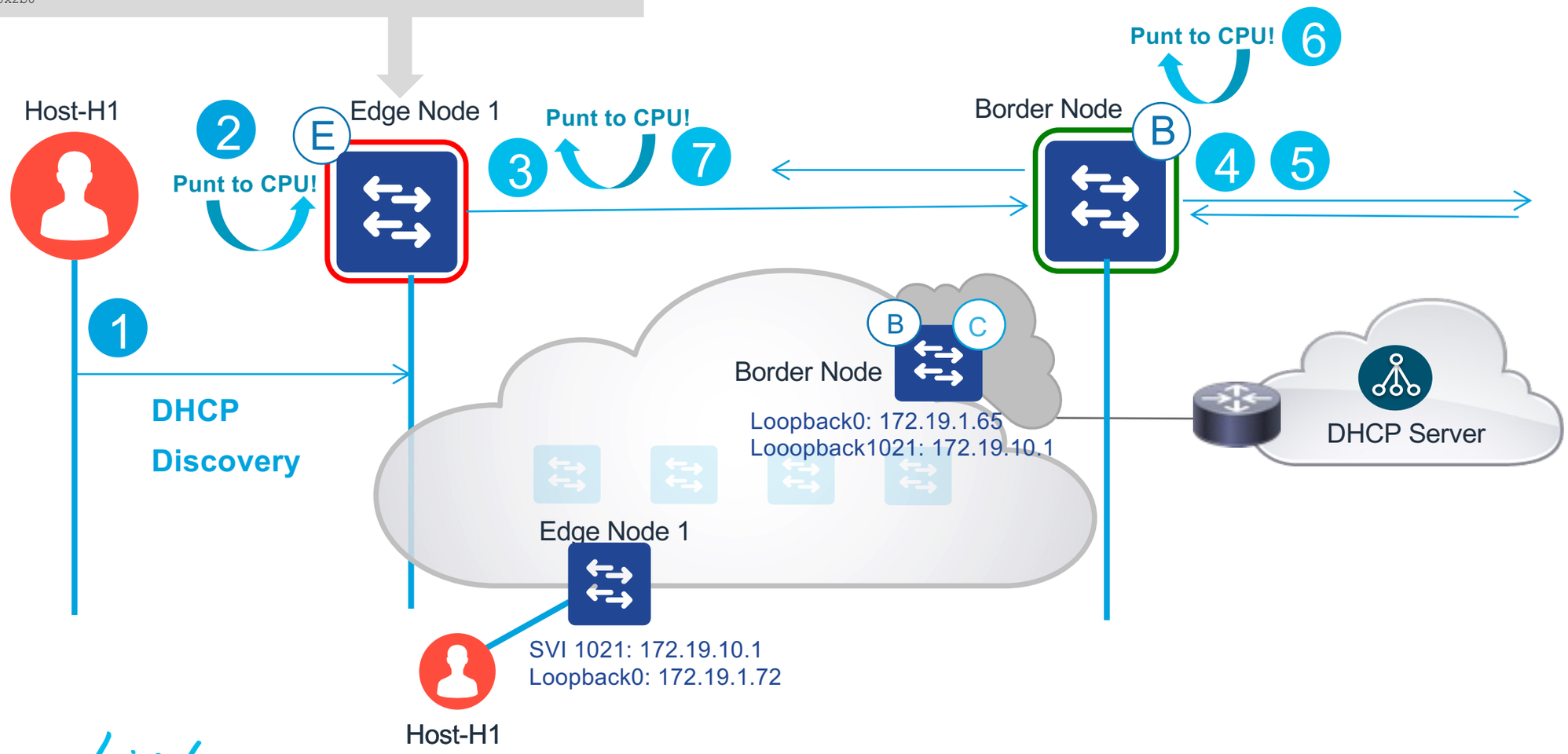
- DHCP offer is encapsulated in VXLAN with Destination RLOC =172.19.1.72



Life of a DHCP Packet [Offer]

```
# EPC CPU Capture in Edge (Punted Packet)
Edge1#show monitor capture cap buffer display-filter bootp.type==2
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

 1656   6.894423 172.19.254.2 -> 172.19.10.1  DHCP 381 DHCP Offer    - Transaction
ID 0x2b0
```

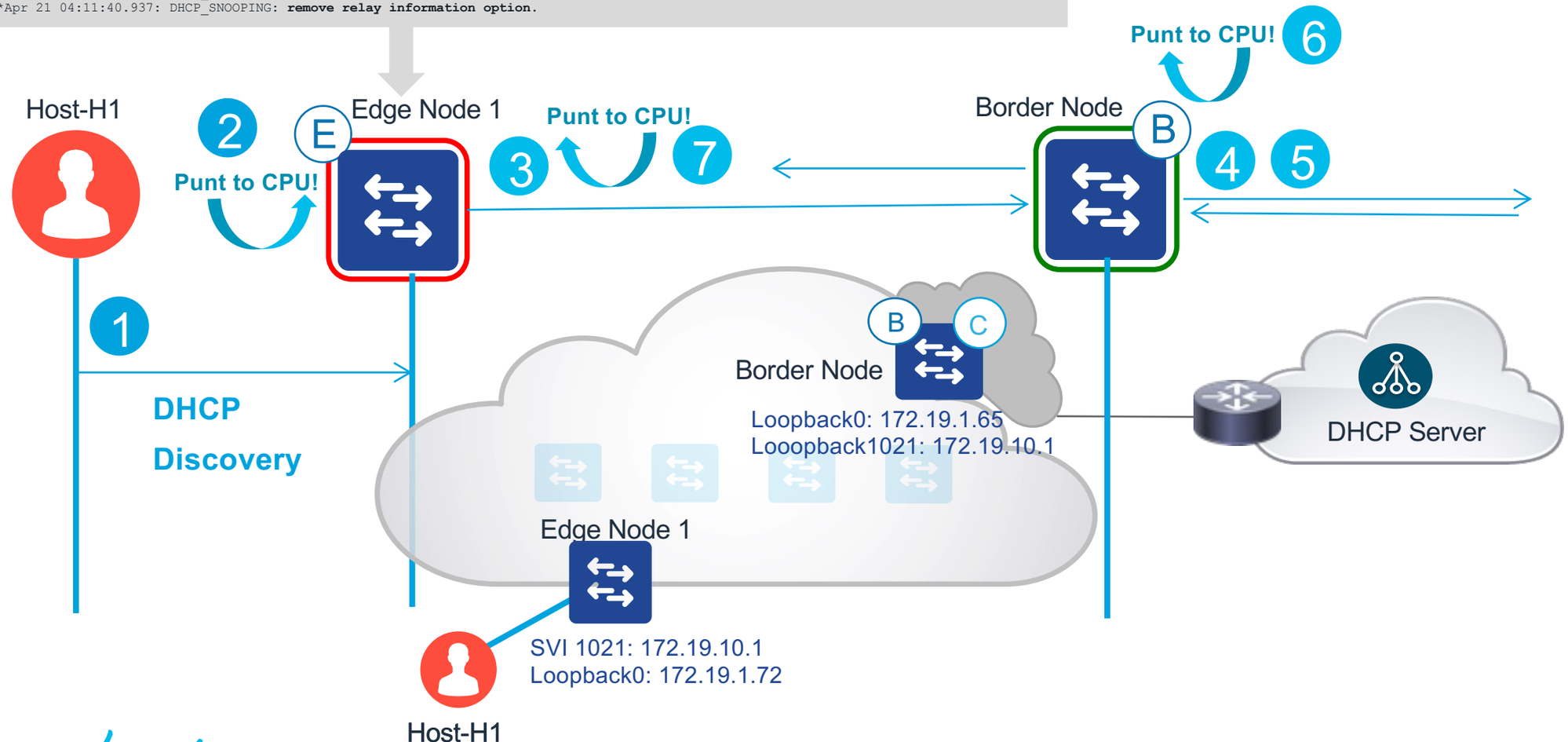
- The VXLAN encapsulated packet is received by Edge Node 1
- After the VXLAN header is removed, DHCP offer packet destined to the SVI IP 172.19.10.1 is punted to the CPU (For-Us Data)



Life of a DHCP Packet [Offer]

```
#debug ip dhcp snooping packet -truncated-

010373: *Apr 21 04:11:40.936: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan1021)
010375: *Apr 21 04:11:40.936: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Vl1021, MAC da:
ffff.ffff.ffff, MAC sa: 0000.0c9f.f45c, IP da: 255.255.255.255, IP sa: 172.19.10.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 172.19.10.30, DHCP
siaddr: 0.0.0.0, DHCP giaddr: 172.19.10.1, DHCP chaddr: d4e8.801f.4876, efp_id: 0, vlan_id: 1021, bootpflag:0x32768(Broadcast)

010380: *Apr 21 04:11:40.937: DHCP_SNOOPING: opt82 data indicates local packet
010381: *Apr 21 04:11:40.937: DHCP_SNOOPING: remove relay information option.
```

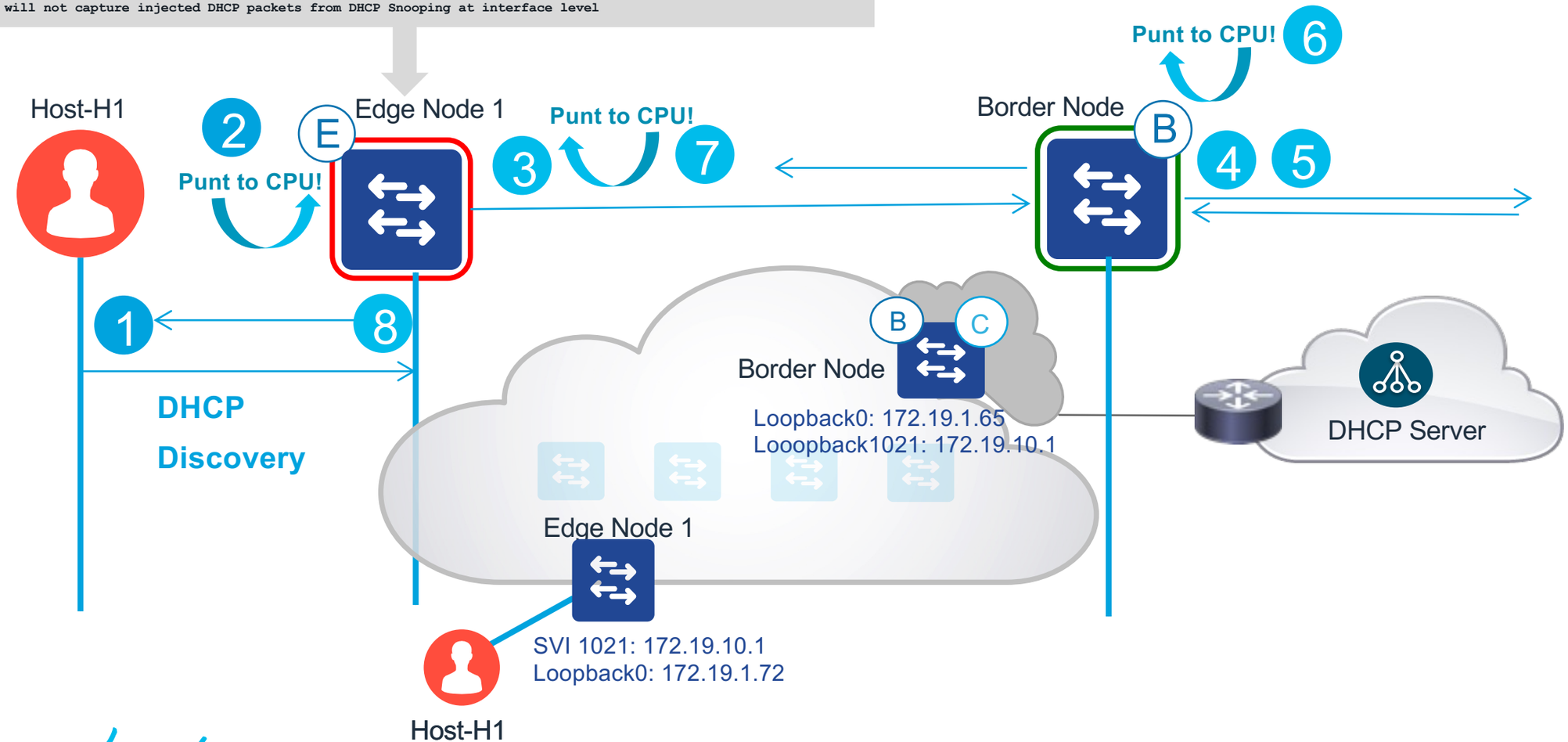
- Option 82 is evaluated again, and the Edge identifies itself as the owner.



Life of a DHCP Packet [Offer]

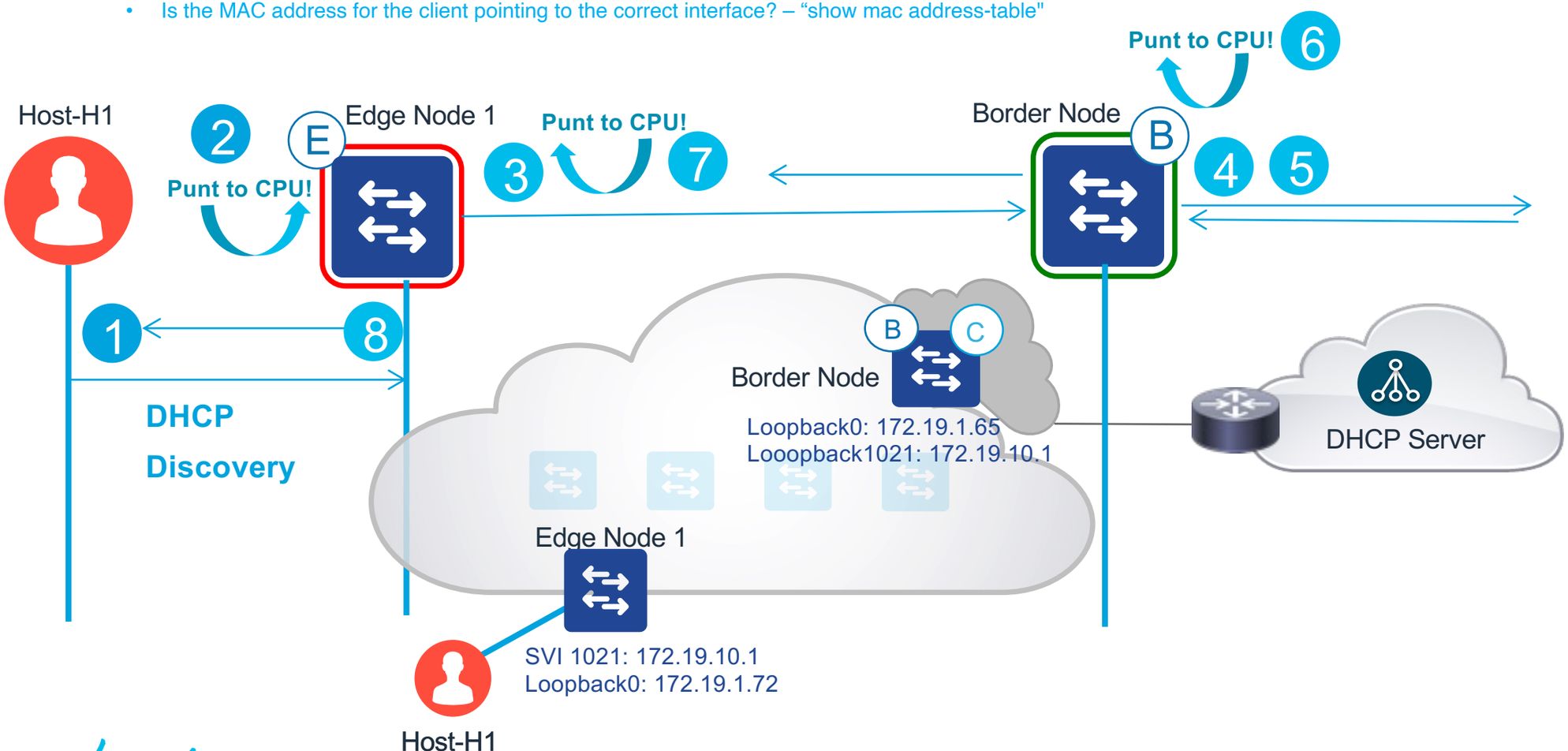
```
#debug ip dhcp snooping packet -truncated-

010390: *Apr 21 04:11:40.937: DHCPSN: idb Te1/0/4 found for proxy_mac 0000.0000.0000real_mac: d4e8.801f.4876,
has_proxy_mac: TRUE
010391: *Apr 21 04:11:40.937: DHCP_SNOOPING: vlan 1021 after pvlan check
010392: *Apr 21 04:11:40.937: DHCP_SNOOPING: direct forward dhcp replyto output port: TenGigabitEthernet1/0/4.

** Proxy MAC debugs are included in DHCP snooping debugs as part of VM brige mode support in 17.6.2
** EPC will not capture injected DHCP packets from DHCP Snooping at interface level
```

- DHCP Offer is sent out to the client



Life of a DHCP Packet [Offer]

- Troubleshooting steps on Fabric Edge:
  - Is the Offer seen in the DHCP snooping debug? If not, is it seen in CPU Capture?
  - Is the Offer coming for a Discover with Unicast Flag or Broadcast Flag set?
  - If Unicast Flag is set, the switch will inspect the Client Hardware Address field to identify which port will be used to forward the Offer
  - Is the MAC address for the client pointing to the correct interface? – “show mac address-table"

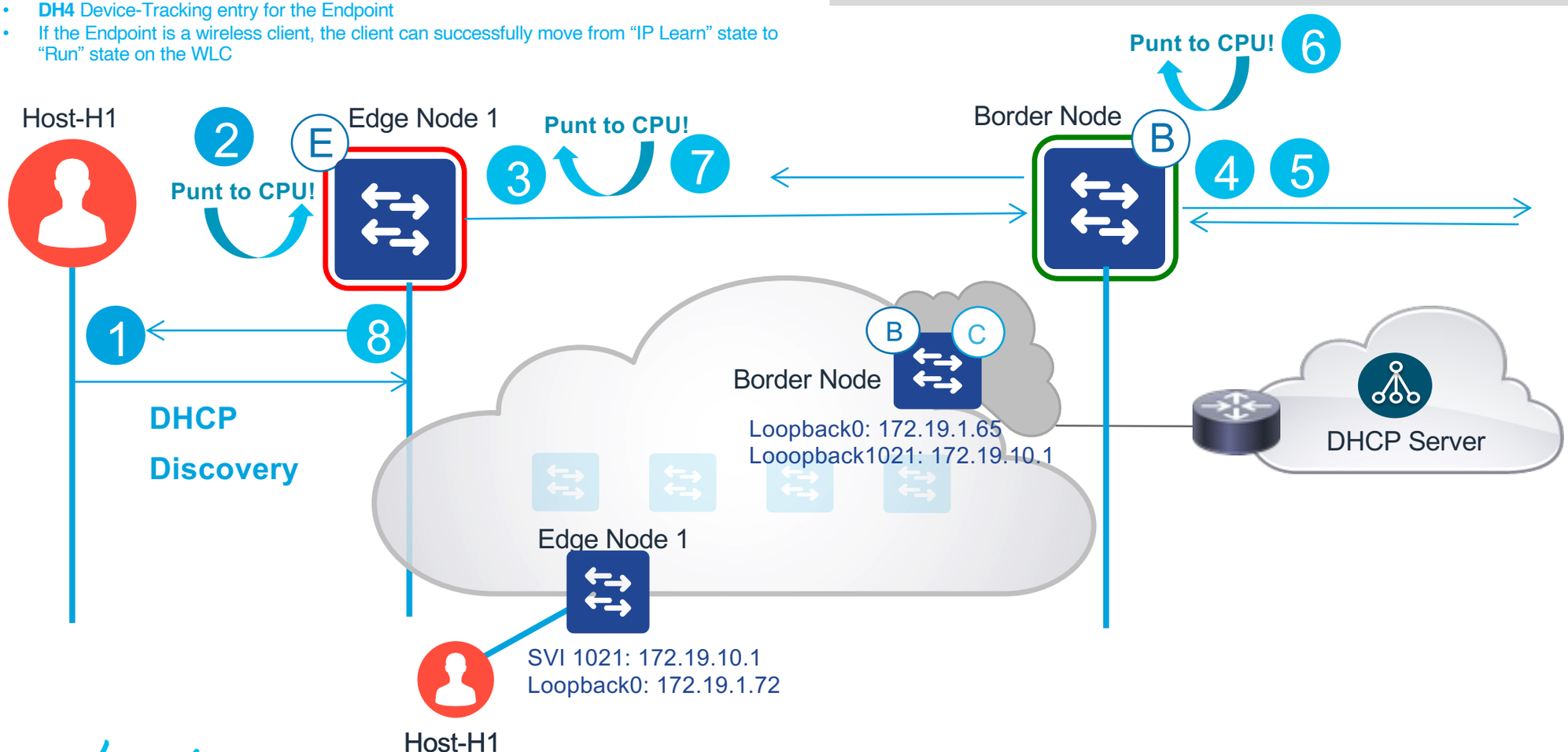


Life of a DHCP Packet [Request & Acknowledge]

- The DHCP Request follows the exact same path and logic as the DHCP Discover
- The DHCP Acknowledge follows the exact same path and logic as the DHCP Offer
- After the DHCP Acknowledge is processed by the Edge, the following entries are created:
  - **DHCP Snooping Binding** entry
  - **DH4** Device-Tracking entry for the Endpoint
  - If the Endpoint is a wireless client, the client can successfully move from "IP Learn" state to "Run" state on the WLC

```
Edge1#show ip dhcp snooping binding int te1/0/4
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
D4:E8:80:1F:48:76   172.19.10.30     86222       dhcp-snooping  1021  TenGigabitEthernet1/0/4
```

```
Edge1#show device-tracking database interface te1/0/4

    Network Layer Address                Link Layer Address     Interface  vlan       prlvl      age        state      Time left
DH4 172.19.10.30                         d4e8.801f.4876         Te1/0/4    1021       0024       3mn        REACHABLE  44 s(86193 s)
```



Life of a DHCP Packet – More Commands

```
Edge1#show platform dhcpsnooping client stats d4e8.801f.4876
DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver
<MessageType>(B): Dhcp message's response expected as 'B'roadcast
<MessageType>(U): Dhcp message's response expected as 'U'nicast
Packet Trace for client MAC D4E8.801F.4876:
Timestamp               Destination MAC  Destination Ip  VLAN  Message      Handler:Action
----------------------- ---------------- --------------- ----  ------------ ----------------
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) PUNT:RECEIVED
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) PUNT:TO_DHCPSN
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) BRIDGE:RECEIVED
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) BRIDGE:TO_DHCPD
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) BRIDGE:TO_INJECT
2022/04/21 07:03:27.306  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPDISCOVER(B) L2INJECT:TO_FWD
2022/04/21 07:03:27.306  BA25.CDF4.AD38   172.19.254.2    0    DHCPDISCOVER(B) INJECT:RECEIVED
2022/04/21 07:03:27.306  BA25.CDF4.AD38   172.19.254.2    0    DHCPDISCOVER(B) INJECT:TO_L2FWD
2022/04/21 07:03:27.314  FFFF.FFFF.FFFF   172.19.10.1     1021 DHCPOFFER(B)    PUNT:RECEIVED
2022/04/21 07:03:27.314  0100.0CCC.CCCC   255.255.255.255 0    DHCPOFFER(B)    INJECT:RECEIVED
2022/04/21 07:03:27.314  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPOFFER(B)    INTERCEPT:RECEIVED
2022/04/21 07:03:27.314  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPOFFER(B)    INTERCEPT:TO_DHCPSN
2022/04/21 07:03:27.316  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  PUNT:RECEIVED
2022/04/21 07:03:27.317  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  PUNT:TO_DHCPSN
2022/04/21 07:03:27.317  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  BRIDGE:RECEIVED
2022/04/21 07:03:27.317  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  BRIDGE:TO_DHCPD
2022/04/21 07:03:27.317  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  BRIDGE:TO_INJECT
2022/04/21 07:03:27.317  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPREQUEST(B)  L2INJECT:TO_FWD
2022/04/21 07:03:27.317  0000.0000.0000   172.19.254.2    0    DHCPREQUEST(B)  INJECT:RECEIVED
2022/04/21 07:03:27.317  0000.0000.0000   172.19.254.2    0    DHCPREQUEST(B)  INJECT:TO_L2FWD
2022/04/21 07:03:27.319  FFFF.FFFF.FFFF   172.19.10.1     1021 DHCPACK(B)      PUNT:RECEIVED
2022/04/21 07:03:27.319  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INJECT:RECEIVED
2022/04/21 07:03:27.319  FFFF.FFFF.FFFF   255.255.255.255 0    DHCPACK(B)      INTERCEPT:RECEIVED
2022/04/21 07:03:27.319  FFFF.FFFF.FFFF   255.255.255.255 1021 DHCPACK(B)      INTERCEPT:TO_DHCPSN
```

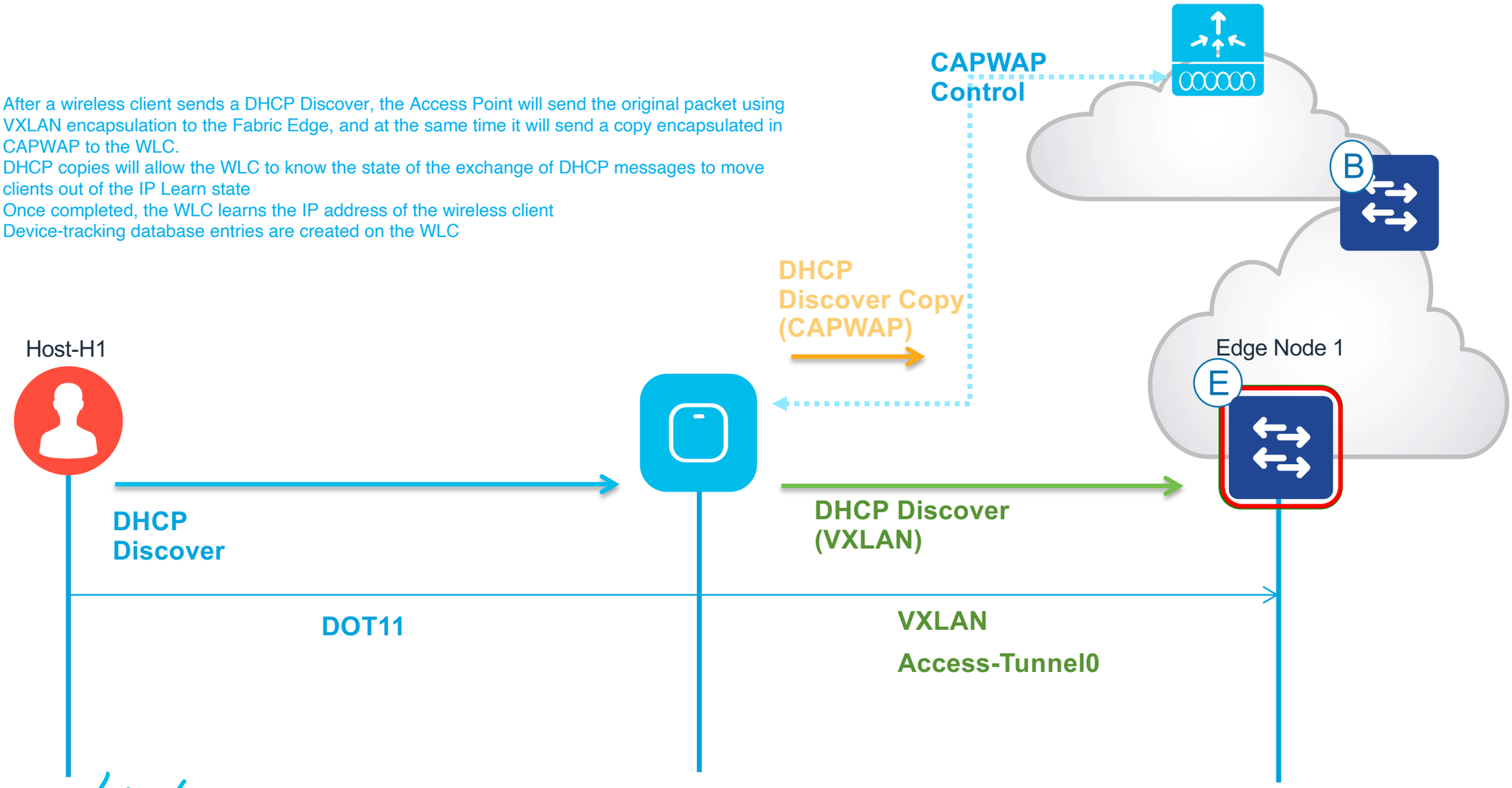
Host-H1

The bridge to possible

DHCP in Fabric Enabled Wireless

Fabric Enabled Wireless

- After a wireless client sends a DHCP Discover, the Access Point will send the original packet using VXLAN encapsulation to the Fabric Edge, and at the same time it will send a copy encapsulated in CAPWAP to the WLC.
- DHCP copies will allow the WLC to know the state of the exchange of DHCP messages to move clients out of the IP Learn state
- Once completed, the WLC learns the IP address of the wireless client
- Device-tracking database entries are created on the WLC



Fabric Enabled Wireless – Catalyst 9800 WLC

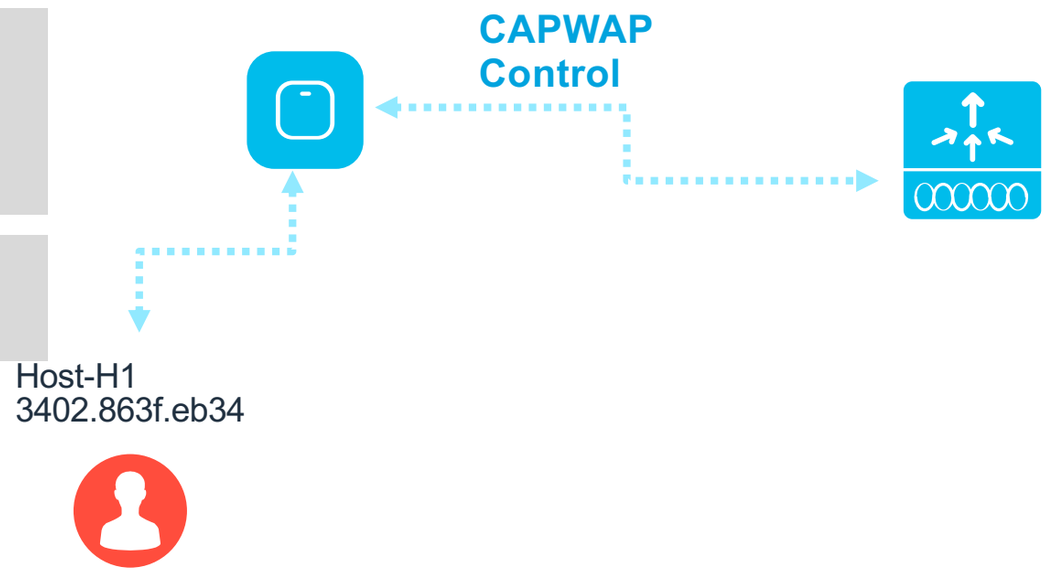
```
WLC#show wireless client summary | i eb34
3402.863f.eb34 AP-9130-CALO-3                    WLAN 18   IP Learn 11ac     None       Local
```

```
WLC#show wlan id 18
WLAN Profile Name     : SanAngelOp_San An_F_83d25043
================================================
Identifier                                : 18
Description                               :
Network Name (SSID)                       : San Angel Open
```

```
WLC#show wireless client mac 3402.863f.eb34 detail | se Fabric
Fabric status : Enabled
  RLOC     : 172.19.1.72
  VNID     : 8188
  SGT      : 0
  Control plane name  : default-control-plane
```

```
WLC#show wireless tag policy detailed PT_Mexic_SanAn_FloorA_bbcb6

Policy Tag Name : PT_Mexic_SanAn_FloorA_bbcb6
Description     : PolicyTagName PT_Mexic_SanAn_FloorA_bbcb6

Number of WLAN-POLICY maps: 5
WLAN Profile Name                Policy Name
-------------------------------------------------------------------------------
SanAngelOp_San An_F_83d25043     SanAngelOp_San An_F_83d25043
```

```
WLC#show run | section 83d25043
wireless profile policy "SanAngelOp_San An_F_83d25043"
 aaa-override
 no central dhcp --!!!!!!!!!!
 no central switching
```

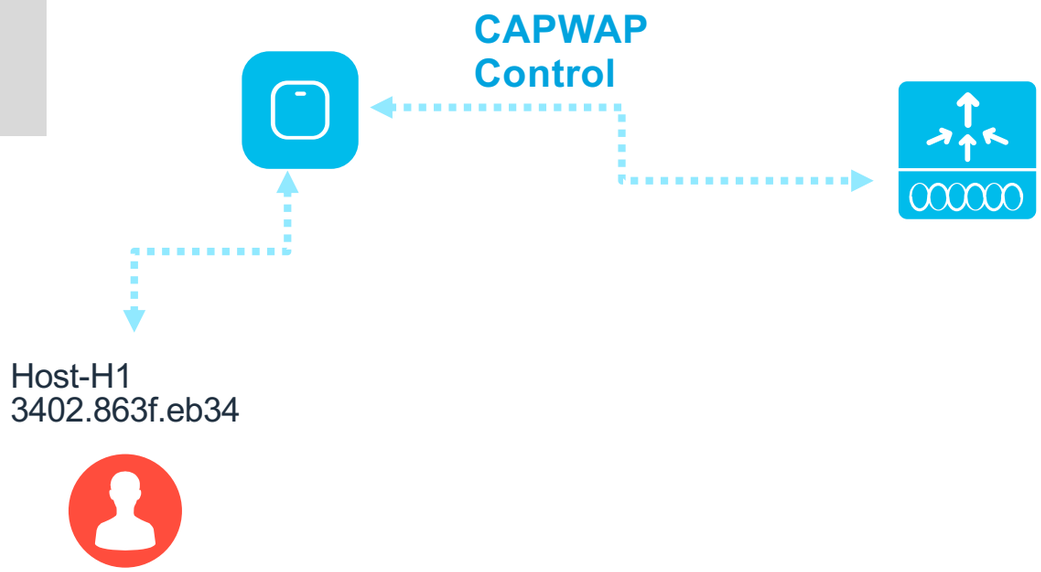


Fabric Enabled Wireless – Access Point

```
AP-9130-CALO-3#show controllers dot11Radio 0 wlan    -- (Check both radios)
wifi0     Link encap:Ethernet  HWaddr A4:B2:39:02:DF:80
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:471 dropped:864 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:2699
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

radio vap id              mac           ssid state
    0      0 A4:B2:39:02:DF:80 San Angel Open    UP

  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr0v0      0    0     0       0      0      0      0    0     0       0     0  2.200000

Vlan BSSID Pri/U/M EncryPolicy Key0 Key1 Key2 Key3 iGTK          SSIDs MFP
   -  DF80   6 6 6       NONE                      DIS San Angel Open   0

VAP-ID           SSID   Bridging Type
     0 San Angel Open Fabric-Tunneled
```

```
AP-9130-CALO-3#show ip tunnel fabric   --- Only created after a client joins
Fabric GWs Information:
Tunnel-Id       GW-IP           GW-MAC        Adj-Status Encap-Type Packet-In  Bytes-In Packet-Out Bytes-out
        1 172.19.1.72 00:00:0C:9F:F3:3A          Forward      VXLAN   1901857 115298412      26704   3313866
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

```
AP-9130-CALO-3#configure ap client-trace filter dhcp enable
AP-9130-CALO-3#terminal monitor
AP-9130-CALO-3#config ap client-trace start

[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:C] DHCP_DISCOVER : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:C] DHCP_DISCOVER : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <wired0> [U:E] DHCP_DISCOVER : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <wired0> [D:C] DHCP_OFFER : TransId 0x5d8867c8
[AP-9130-CALO-3] [00:00:0c:9f:f4:5c] <wired0> [U:C] DHCP_OFFER : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [D:W] DHCP_OFFER : TransId 0x5d8867c8
[AP-9130-CALO-3] [00:00:0c:9f:f4:5c] <wired0> [U:E] DHCP_OFFER : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:W] DOT11_ACTION : Block Ack - ADDBA Response, TID: 6
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:W] DHCP_REQUEST : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:C] DHCP_REQUEST : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [U:C] DHCP_REQUEST : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <wired0> [U:E] DHCP_REQUEST : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <wired0> [D:C] DHCP_ACK : TransId 0x5d8867c8
[AP-9130-CALO-3] [00:00:0c:9f:f4:5c] <wired0> [U:C] DHCP_ACK : TransId 0x5d8867c8
[AP-9130-CALO-3] [34:02:86:3f:eb:34] <aprlv0> [D:W] DHCP_ACK : TransId 0x5d8867c8
[AP-9130-CALO-3] [00:00:0c:9f:f4:5c] <wired0> [U:E] DHCP_ACK : TransId 0x5d8867c8

AP-9130-CALO-3#config ap client-trace stop
```



Fabric Enabled Wireless – Fabric Edge

```
Edge1#show mac address-table | i 3402.863f.eb34
1021    3402.863f.eb34    CP_LEARN    Ac1

Edge1#show vlan id 1021 | i active
1021 172_19_10_0-Campus              active    L2LI0:8188, Te1/0/4,

Edge1#show lisp instance-id 8188 ethernet database wlc clients  detail

WLC clients/access-points information for router lisp 0 IID 8188

Hardware Address: 3402.863f.eb34
Type:             client
Sources:          1
Tunnel Update:    Signalled
Source MS:        172.19.1.67
RLOC:             172.19.1.72
Up time:          00:16:11
Metadata length:  34
Metadata (hex):   00 01 00 22   00 01 00 0C   AC 13 05 07   00 00 10 01
                  00 02 00 06   00 00 00 03   00 0C 00 00   00 00 62 61
                  06 9E
```

```
Edge1#show access-tunnel summary


Name    RLOC IP(Source)  AP IP(Destination)  VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------
Ac1     172.19.1.72      172.19.5.7          0       N/A          4789
```

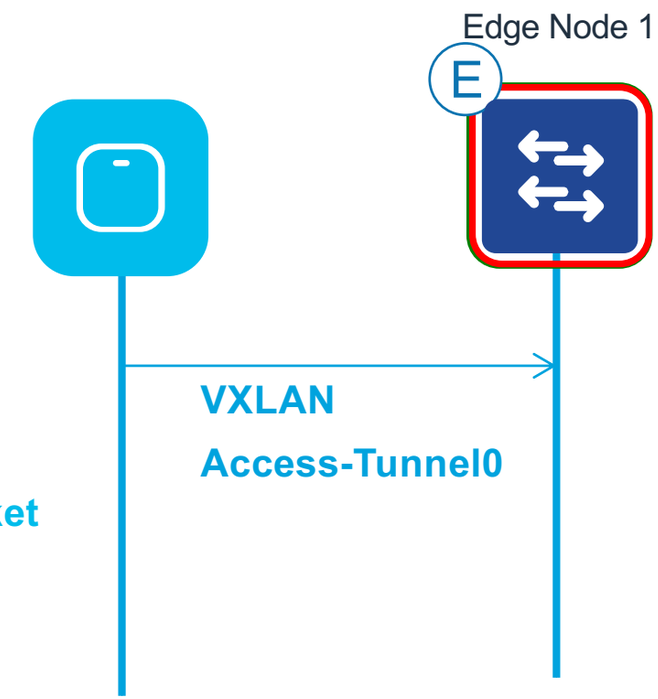
```
Edge1#show device-tracking data add 172.19.5.7

    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      age        state      Time left
DH4 172.19.5.7                             6c71.0df4.28ec         Te1/0/24   2045       0024       6s         REACHABLE  244 s(78032 s)

Edge1#show cdp nei te1/0/24
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
AP-9130-CALO-3   Ten 1/0/24        164              R T   C9130AXI- Gig 0
```

```
Edge1#show pla software fed switch active matm macTable vlan 1021 mac 3402.863f.eb34
VLAN   MAC                Type  Seq#    EC_Bi  Flags  machandle          siHandle           riHandle           diHandle
*a_time  *e_time  ports                         Con
-------------------------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------
1021   3402.863f.eb34   0x840101    3682      0     64  0x7ff9c141b4c8     0x7ff9c13c8ab8     0x7ff9c10114d8     0x0
0        0  Ac1                            No
```

```
Edge1#show monitor capture cap buffer display-fiter bootp.type==1
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

87  12.299177      0.0.0.0 -> 255.255.255.255 DHCP 422 DHCP Discover - Transaction ID 0x24377b81
   88  12.299215      0.0.0.0 -> 255.255.255.255 DHCP 394 DHCP Discover - Transaction ID 0x24377b81

Edge1#show monitor capture cap buffer display-fiter "bootp.type==1 and udp.port==5247"
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

87      12.299177      0.0.0.0 -> 255.255.255.255 DHCP 422 DHCP Discover - Transaction ID 0x24377b81  --CAPWAP!

Edge1#show monitor capture cap buffer display-fiter "bootp.type==1 and vxlan
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

88  12.299215      0.0.0.0 -> 255.255.255.255 DHCP 394 DHCP Discover - Transaction ID 0x24377b81 - VXLAN!
```

Which one is used for forwarding???

```
090589: *Apr 21 07:48:29.547: DHCP_SNOOPING: received new DHCP packet from input interface (AccessTunnel1)
090590: *Apr 21 07:48:29.548: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Ac1, MAC da:
ffff.ffff.ffff, MAC sa: 3402.863f.eb34, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr:
0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 3402.863f.eb34, efp_id: 0, vlan_id: 1021, bootpflag:0x32768(Broadcast)
```



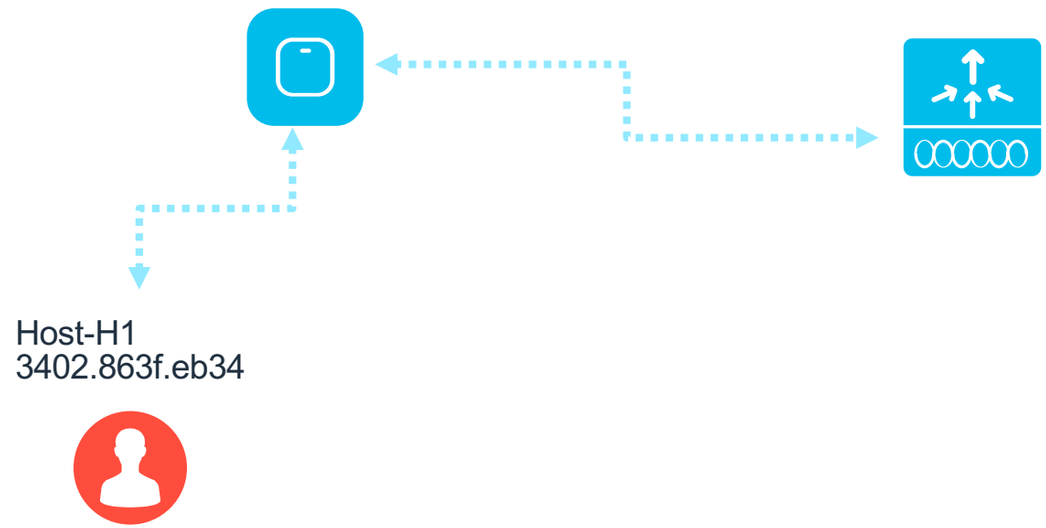
The DHCP packet handling after the packet is received from the Access-tunnel, is exactly the same as in wired case

Fabric Enabled Wireless – Fabric Edge

```
WLC#debug wireless mac 3402.863f.eb34 internal to-file flash:DHCP

WLC#more flash:DHCP | i SISF_DHCP
2022/04/21 07:54:00.045899 {wncd_x_R0-0}{2}: [sisf-parser] [27836]: (debug): capwap_9000000c vlan 1     Cached Option 53: SISF_DHCPDISCOVER
2022/04/21 07:54:00.045914 {wncd_x_R0-0}{2}: [sisf-packet] [27836]: (info): RX: DHCPv4 from interface capwap_9000000c on vlan 1 Src MAC: 3402.863f.eb34 Dst MAC: ffff.ffff.ffff src_ip:
0.0.0.0, dst_ip: 255.255.255.255, BOOTPREQUEST, SISF_DHCPDISCOVER, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 3402.863f.eb34
2022/04/21 07:54:00.049361 {wncd_x_R0-0}{2}: [sisf-parser] [27836]: (debug): capwap_9000000c vlan 1     Cached Option 53: SISF_DHCPOFFER
2022/04/21 07:54:00.049374 {wncd_x_R0-0}{2}: [sisf-packet] [27836]: (info): RX: DHCPv4 from interface capwap_9000000c on vlan 1 Src MAC: 0000.0c9f.f45c Dst MAC: ffff.ffff.ffff src_ip:
172.19.10.1, dst_ip: 255.255.255.255, BOOTPREPLY, SISF_DHCPOFFER, giaddr: 172.19.10.1, yiaddr: 172.19.10.2, CMAC: 3402.863f.eb34
2022/04/21 07:54:00.053785 {wncd_x_R0-0}{2}: [sisf-parser] [27836]: (debug): capwap_9000000c vlan 1     Cached Option 53: SISF_DHCPREQUEST
2022/04/21 07:54:00.053797 {wncd_x_R0-0}{2}: [sisf-packet] [27836]: (info): RX: DHCPv4 from interface capwap_9000000c on vlan 1 Src MAC: 3402.863f.eb34 Dst MAC: ffff.ffff.ffff src_ip:
0.0.0.0, dst_ip: 255.255.255.255, BOOTPREQUEST, SISF_DHCPREQUEST, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 3402.863f.eb34
2022/04/21 07:54:00.057731 {wncd_x_R0-0}{2}: [sisf-parser] [27836]: (debug): capwap_9000000c vlan 1     Cached Option 53: SISF_DHCPACK
2022/04/21 07:54:00.057744 {wncd_x_R0-0}{2}: [sisf-packet] [27836]: (info): RX: DHCPv4 from interface capwap_9000000c on vlan 1 Src MAC: 0000.0c9f.f45c Dst MAC: ffff.ffff.ffff src_ip:
172.19.10.1, dst_ip: 255.255.255.255, BOOTPREPLY, SISF_DHCPACK, giaddr: 172.19.10.1, yiaddr: 172.19.10.2, CMAC: 3402.863f.eb34
```

```
WLC#show wireless client mac-address 3402.863f.eb34 detail  | i IP|Learn|DHCP
Client IPv4 Address : 172.19.10.2
Client IPv6 Addresses : fe80::1da8:3730:6cf4:f23b
Last Policy Manager State : IP Learn Complete
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
  Protocol Map     : 0x000029  (OUI, DHCP, HTTP)
  Device Protocol  : DHCP
```

```
WLC#show wireless device-tracking database ip 172.19.10.2
  IP                                      ZONE-ID     STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------------------
  172.19.10.2                             0x00000000  Reachable   IPv4 DHCP   3402.863f.eb34
```



PXE Considerations and Limitations

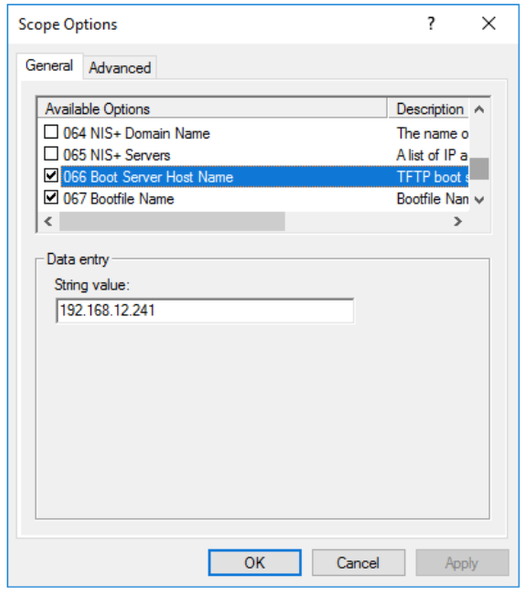
PXE Considerations and Limitations

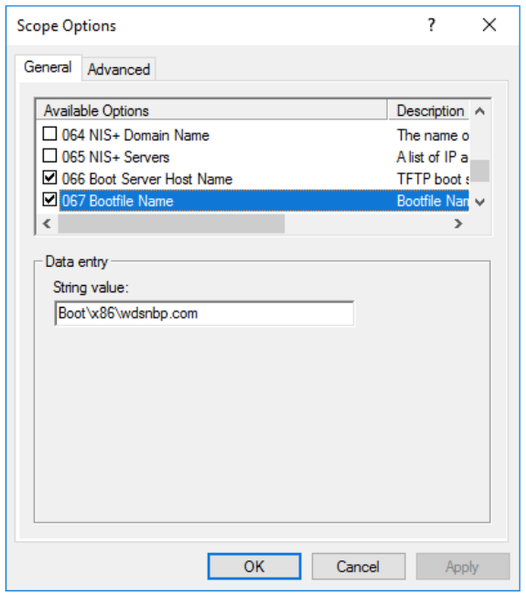
- **PXE Boot Servers and IP Helpers**

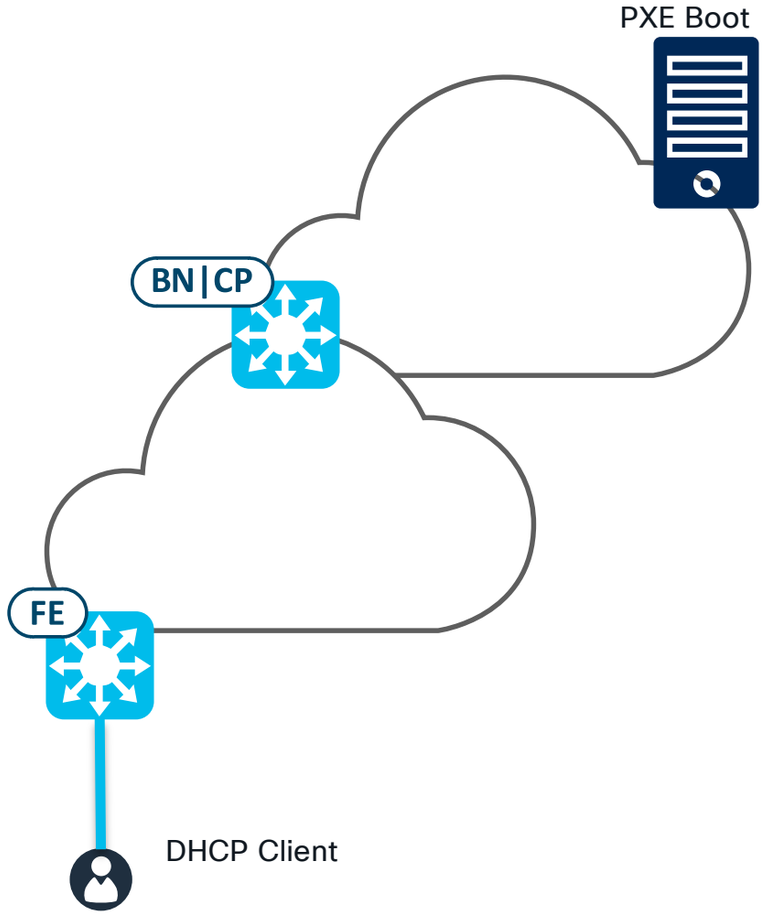
Using IP Helper addresses (Relays) is often suggested for PXE environments to forward broadcast UDP packets (usually TFTP) to PXE servers.

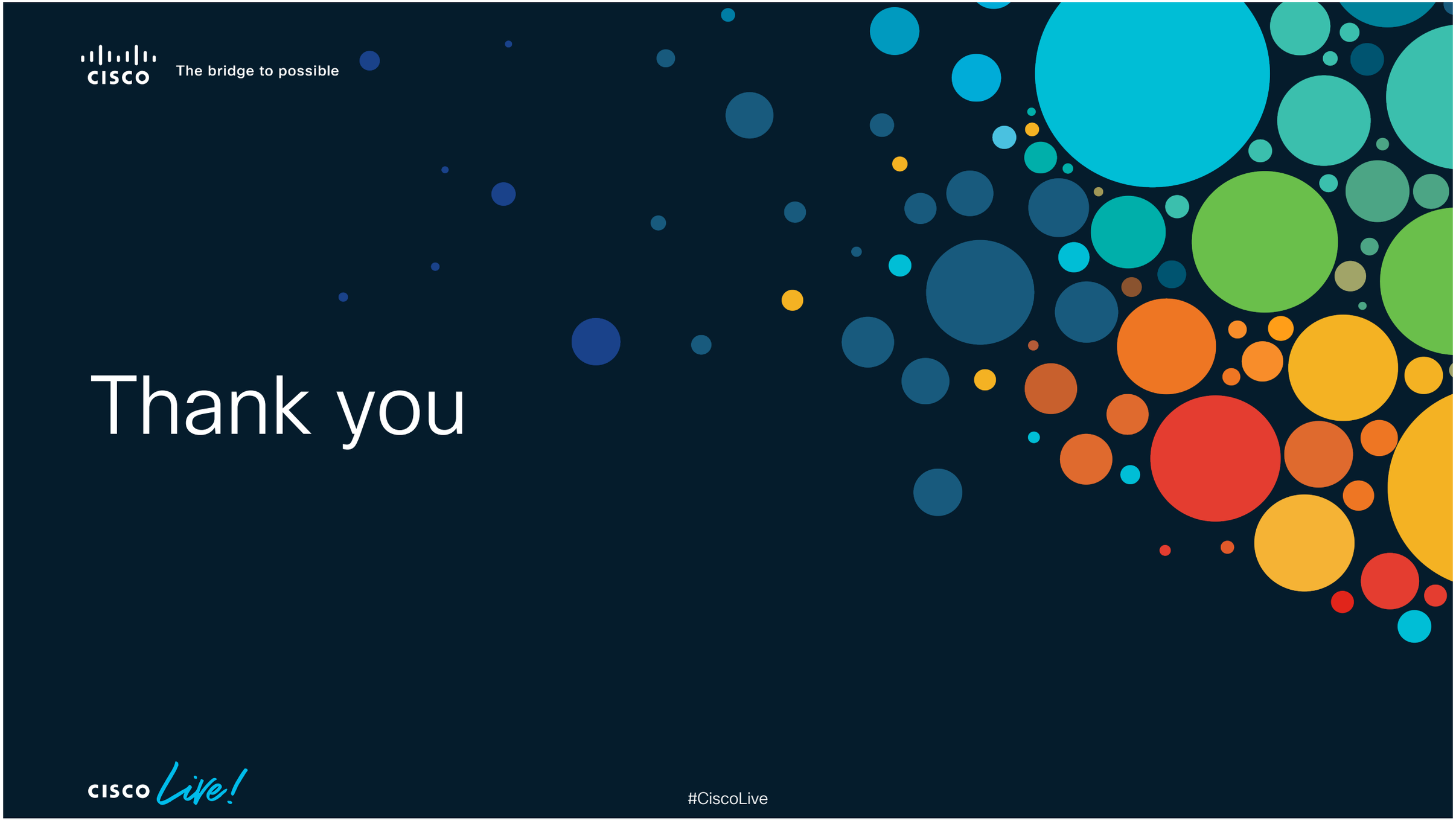
In an SDA Fabric environment (and any other distributed Anycast-Gateway network), this approach does not work as the source IP of the PXE relay is the Anycast Gateway IP.

- **Use Option 66 and 67 instead**








cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive

#CiscoLive