Cisco SD-Access Fabric Edge DHCP Process/Packet Flow and Decoding

Revised: September 10, 2019

Introduction

This guide explains how to troubleshoot the Cisco SD-Access fabric edge DHCP process.

Host DHCP Onboarding Process

Fabric edge 1 (FE1) should have the following configs pushed from Cisco DNA Center:

```
ip dhcp relay information option
ip dhcp snooping vlan 3000   --> Note: All new Cisco DNA Center releases send VLAN starting from 1021. Old
method of VLAN 3000 is not applicable.
ip dhcp snooping
```

Verify **show run | i dhcp**. If you see **no dhcp service**, make sure this is reenabled, or the DHCP relay function will not work and DHCP packets will not leave the fabric edge. In addition, **debug ip dhcp server packet** will not produce any output.

Verify that udp:67 is open and listening via **show udp**.

Note that some older documents state that the following settings also are configured. Do not use them.

- ip dhcp relay source-interface

```
interface vlan 3000-3001   --> Note: All new Cisco DNA Center releases send VLAN starting from 1021. Old
method of VLAN 3000 is not applicable.
 ip dhcp relay source-interface Loopback0
!
```

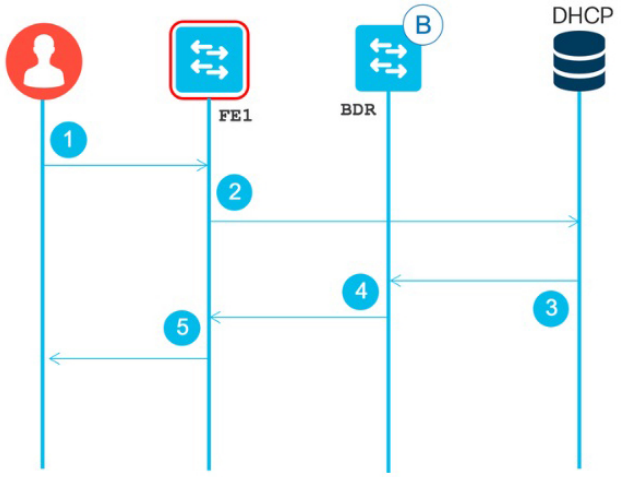
Note When this setting is configured, the DHCP relay agent puts the Loopback0 address as relay agent address (giaddr), which breaks the campus fabric solution.

- ip dhcp relay information option vpn

```
ip dhcp relay information option vpn
```

Note When this setting is configured, the DHCP server inserts additional suboptions (150, 151, and 152) in option 82. This format breaks the campus fabric solution when the DHCP server is located outside a campus fabric.

Fabric Edge DHCP Process Flow



1. The DHCP client generates a DHCP request and broadcasts it on the network
2. FE uses DHCP Snooping to add it's RLOC as the remote ID in Option 82 and sets giaddress as the Anycast SVI address

   Using DHCP Relay the request is forwarded to the Border
3. DHCP Server replies with offer to Anycast SVI address
4. Border uses the remote ID in option 82 to forward the packet
5. FE installs the DHCP binding and forwards the reply to client

Validate the Fabric Edge (FE1) DHCP Binding

```
FE1# show ip dhcp snooping binding
MacAddress             IpAddress          Lease(sec)   Type             VLAN     Interface
------------------     ---------------    ----------   ------------     ----     --------------------
00:0C:29:DE:32:40      192.168.101.45     689128       dhcp-snooping    3000     TenGigabitEthernet6/0/7
Total number of bindings: 1
```

Fabric Edge Configs Pushed from Cisco DNA Center

```
vlan 3000    --> Note: All new Cisco DNA Center releases send VLAN starting from 1021. Old method of VLAN 3000
 is not applicable.
 name 192_168_101_0-VRF1
!
vlan 3001
 name 192_168_102_0-VRF1
!
interface Loopback0
 ip address 192.168.1.6 255.255.255.255
 ip router isis sdaccess
!
interface LISP0
!
interface LISP0.4097
!
interface LISP0.4098
!
interface Vlan3000
 description Configured from apic-em
 mac-address 0000.0c9f.fc17
 vrf forwarding VRF1
 ip address 192.168.101.1 255.255.255.0
 ip helper-address 192.168.103.2 --> Note that the "global" keyword has been removed. DHCP discovery goes
through the overlay.
 ip route-cache same-interface
```

```
 no lisp mobility liveness test  ---> Old Cisco DNA Center (2.0.0.3106) doesn't configure it. Make sure it is
 configured.
 lisp mobility 192_168_101_0-VRF1
!
interface Vlan3001
 description Configured from apic-em
 mac-address 0000.0c9f.fc18
 vrf forwarding VRF1
 ip address 192.168.102.1 255.255.255.0
 ip helper-address 192.168.103.2
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test  ---> Old Cisco DNA Center (2.0.0.3106) doesn't configure it. Make sure it is
 configured.
 lisp mobility 192_168_102_0-VRF1
!
router lisp
 locator-table default
 locator-set rloc_ba2d01d9-3ad5-4829-a326-8fa2828ac1d0
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator default-set rloc_ba2d01d9-3ad5-4829-a326-8fa2828ac1d0
 service ipv4
  encapsulation vxlan
  itr map-resolver 192.168.1.8
  itr
  etr map-server 192.168.1.8 key uci
  etr map-server 192.168.1.8 proxy-reply
  etr
  sgt
  exit-service-ipv4
 !
 service ethernet
  itr map-resolver 192.168.1.8
  itr
  etr map-server 192.168.1.8 key uci
  etr map-server 192.168.1.8 proxy-reply
  etr
  exit-service-ethernet
 !
 instance-id 4097
  service ipv4
   eid-table vrf DEFAULT_VN
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4098
  dynamic-eid 192_168_101_0-VRF1
   database-mapping 192.168.101.0/24 locator-set rloc_ba2d01d9-3ad5-4829-a326-8fa2828ac1d0
   exit-dynamic-eid
  !
  dynamic-eid 192_168_102_0-VRF1
   database-mapping 192.168.102.0/24 locator-set rloc_ba2d01d9-3ad5-4829-a326-8fa2828ac1d0
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf VRF1
   exit-service-ipv4
  !
  exit-instance-id
 !
 exit-router-lisp
```

```
!
router isis sdaccess
 net 77.0001.0000.0000.0006.00
 metric-style wide
!
```

Other Useful CLI Commands to Verify Host Onboarding

```
Edge1# show mac address-table
         Mac Address Table
-------------------------------------------

Vlan   Mac Address      Type       Ports
----   -----------      --------   -----
...
All    ffff.ffff.ffff    STATIC     CPU
  1    0042.5aeb.48c7    STATIC     Vl1
3000   0000.0c9f.fc17    STATIC     Vl3000
3000   000c.29de.3240    DYNAMIC    Te6/0/7
3001   0000.0c9f.fc18    STATIC     Vl3001
Total Mac Addresses for this criterion: 25
Edge1#

Edge1# show arp vrf VRF1
Protocol Address         Age (min) Hardware Addr    Type   Interface
Internet 192.168.101.1       -     0000.0c9f.fc17   ARPA   Vlan3000
Internet 192.168.102.1       -     0000.0c9f.fc18   ARPA   Vlan3001
Edge1#

Edge1# show device-tracking database
Binding Table has 4 entries, 2 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6
 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated   0100:Statically assigned

Network Layer Address           Link Layer Address Interface  vlan  prlvl  age   state      Time left
L   192.168.102.1               0000.0c9f.fc18 Vl3001         3001  0100   34mn  DOWN
DH4 192.168.101.45              000c.29de.3240 Te6/0/7        3000  0025   119s  REACHABLE  186 s(695581 s)
L   192.168.101.1               0000.0c9f.fc17 Vl3000         3000  0100   73mn  REACHABLE
ND FE80::6954:5B77:F21B:DDA7    000c.29de.3240 Te6/0/7        3000  0005   59s   REACHABLE  246 s try 0

Edge1#

Edge1# show ip lisp eid-table summary
Router-lisp ID:   0
Instance count:   2
Key: DB - Local EID Database entry count (@ - RLOC check pending
                                          * - RLOC consistency problem),
     DB no route - Local EID DB entries with no matching RIB route,
     Cache - Remote EID mapping cache size, IID - Instance ID,
     Role - Configured Role

                     Interface     DB  DB no  Cache  Incom  Cache
EID VRF name             (.IID)  size  route  size   plete  Idle   Role
DEFAULT_VN           LISP0.4097     0    0      1    0.0%   0%     ITR-ETR
VRF1                 LISP0.4098   44@    0     47      2%   0%     ITR-ETR

Number of eid-tables:                              2
Total number of database entries:                  44 (inactive 44)
```

```
EID-tables with inconsistent locators:                1
Total number of map-cache entries:                   48
EID-tables with incomplete map-cache entries:         1
EID-tables pending map-cache update to FIB:           0
Edge1#
```

For the following command, find the .pcap file that saves you the trouble of converting and separating values. The tool is located on DHCP option 82 decoding tool.

For the circuit ID:

```
00040bb80607
00 suboption 1-> Vlan/mod/port
04 length of option
0bb8 -> Vlan 3000 (0xbb8)
06 ->     module 6
07 ->     port 7
```

For the remote ID:

```
030800100201c0a80106

03 -> sub-option LISP
08 -> length of option
001002 -> 4098 in decimals --> LISP Instance ID 4098
01 -> IPV4 locator (IPv6 would be 02)
c0.a8.01.06  -> 192.168.1.6 Source locator (Loopback 0 of xTR)
```

Packet Capture of the DHCP Process on the Host

```
No.  Time                    Delta Time      Source      Destination       Protocol
1    18:57:37.179567000      0.000000000     1.1.1.2     192.168.103.2     DHCP

Length    Info
359       DHCP Discover - Transaction ID 0xae99c7b2

Frame 1: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface 0
Ethernet II, Src: 00:38:df:5d:dc:5a (00:38:df:5d:dc:5a), Dst: Vmware_96:6d:f7 (00:50:56:96:6d:f7)
Internet Protocol Version 4, Src: 1.1.1.2 (1.1.1.2), Dst: 192.168.103.2 (192.168.103.2)
User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)
Bootstrap Protocol (Discover)
   Message type: Boot Request (1)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 1
   Transaction ID: 0xae99c7b2
   Seconds elapsed: 0
   Bootp flags: 0x8000 (Broadcast)
       1... .... .... .... = Broadcast flag: Broadcast
       .000 0000 0000 0000 = Reserved flags: 0x0000
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 0.0.0.0 (0.0.0.0)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 192.168.101.1 (192.168.101.1)
   Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
   Option: (53) DHCP Message Type (Discover)
       Length: 1
       DHCP: Discover (1)
```

```
   Option: (61) Client identifier
       Length: 7
       Hardware type: Ethernet (0x01)
       Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
   Option: (12) Host Name
       Length: 15
       Host Name: DESKTOP-LPMOG6M
   Option: (60) Vendor class identifier
       Length: 8
       Vendor class identifier: MSFT 5.0
   Option: (55) Parameter Request List
       Length: 13
       Parameter Request List Item: (1) Subnet Mask
       Parameter Request List Item: (3) Router
       Parameter Request List Item: (6) Domain Name Server
       Parameter Request List Item: (15) Domain Name
       Parameter Request List Item: (31) Perform Router Discover
       Parameter Request List Item: (33) Static Route
       Parameter Request List Item: (43) Vendor-Specific Information
       Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
       Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
       Parameter Request List Item: (121) Classless Static Route
       Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
       Parameter Request List Item: (252) Private/Proxy autodiscovery
   Option: (82) Agent Information Option
       Length: 20
       Option 82 Suboption: (1) Agent Circuit ID
           Length: 6
           Agent Circuit ID: 00040bb80607
       Option 82 Suboption: (2) Agent Remote ID
           Length: 10
           Agent Remote ID: 030800100201c0a80106
   Option: (255) End
       Option End: 255


No.  Time                 Delta Time     Source           Destination       Protocol
2    18:57:37.179822000   0.000255000    192.168.103.2    192.168.101.1     DHCP

Length    Info
364       DHCP Offer - Transaction ID 0xae99c7b2

Frame 2: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface 0
Ethernet II, Src: Vmware_96:6d:f7 (00:50:56:96:6d:f7), Dst: 00:38:df:5d:dc:5a (00:38:df:5d:dc:5a)
Internet Protocol Version 4, Src: 192.168.103.2 (192.168.103.2), Dst: 192.168.101.1 (192.168.101.1)
User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)
Bootstrap Protocol (Offer)
   Message type: Boot Reply (2)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0xae99c7b2
   Seconds elapsed: 0
   Bootp flags: 0x8000 (Broadcast)
       1... .... .... .... = Broadcast flag: Broadcast
       .000 0000 0000 0000 = Reserved flags: 0x0000
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 192.168.101.45 (192.168.101.45)
   Next server IP address: 192.168.103.2 (192.168.103.2)
   Relay agent IP address: 192.168.101.1 (192.168.101.1)
   Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
```

```
   Magic cookie: DHCP
   Option: (53) DHCP Message Type (Offer)
       Length: 1
       DHCP: Offer (2)
   Option: (1) Subnet Mask
       Length: 4
     Subnet Mask: 255.255.255.0 (255.255.255.0)
   Option: (58) Renewal Time Value
       Length: 4
       Renewal Time Value: (345600s) 4 days
   Option: (59) Rebinding Time Value
       Length: 4
       Rebinding Time Value: (604800s) 7 days
   Option: (51) IP Address Lease Time
       Length: 4
       IP Address Lease Time: (691200s) 8 days
   Option: (54) DHCP Server Identifier
       Length: 4
       DHCP Server Identifier: 192.168.103.2 (192.168.103.2)
   Option: (3) Router
       Length: 4
       Router: 192.168.101.1 (192.168.101.1)
   Option: (6) Domain Name Server
       Length: 4
       Domain Name Server: 171.70.168.183 (171.70.168.183)
   Option: (15) Domain Name
       Length: 12
       Domain Name: fabric1.com
   Option: (82) Agent Information Option
       Length: 20
       Option 82 Suboption: (1) Agent Circuit ID
           Length: 6
           Agent Circuit ID: 00040bb80607
       Option 82 Suboption: (2) Agent Remote ID
           Length: 10
          Agent Remote ID: 030800100201c0a80106
   Option: (255) End
       Option End: 255


No.  Time                 Delta Time      Source      Destination      Protocol
3    18:57:37.183947000   0.004125000     1.1.1.2     192.168.103.2    DHCP

Length    Info
391       DHCP Request - Transaction ID 0xae99c7b2

Frame 3: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on interface 0
Ethernet II, Src: 00:38:df:5d:dc:5a (00:38:df:5d:dc:5a), Dst: Vmware_96:6d:f7 (00:50:56:96:6d:f7)
Internet Protocol Version 4, Src: 1.1.1.2 (1.1.1.2), Dst: 192.168.103.2 (192.168.103.2)
User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)
Bootstrap Protocol (Request)
   Message type: Boot Request (1)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 1
   Transaction ID: 0xae99c7b2
   Seconds elapsed: 0
   Bootp flags: 0x8000 (Broadcast)
       1... .... .... .... = Broadcast flag: Broadcast
       .000 0000 0000 0000 = Reserved flags: 0x0000
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 0.0.0.0 (0.0.0.0)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 192.168.101.1 (192.168.101.1)
   Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
```

```
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
   Option: (53) DHCP Message Type (Request)
       Length: 1
       DHCP: Request (3)
   Option: (61) Client identifier
       Length: 7
       Hardware type: Ethernet (0x01)
       Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
   Option: (50) Requested IP Address
       Length: 4
       Requested IP Address: 192.168.101.45 (192.168.101.45)
   Option: (54) DHCP Server Identifier
       Length: 4
       DHCP Server Identifier: 192.168.103.2 (192.168.103.2)
   Option: (12) Host Name
       Length: 15
       Host Name: DESKTOP-LPMOG6M
   Option: (81) Client Fully Qualified Domain Name
       Length: 18
       Flags: 0x00
       0000 .... = Reserved flags: 0x00
       .... 0... = Server DDNS: Some server updates
       .... .0.. = Encoding: ASCII encoding
       .... ..0. = Server overrides: No override
       .... ...0 = Server: Client
       A-RR result: 0
       PTR-RR result: 0
       Client name: DESKTOP-LPMOG6M
   Option: (60) Vendor class identifier
       Length: 8
       Vendor class identifier: MSFT 5.0
   Option: (55) Parameter Request List
       Length: 13
      Parameter Request List Item: (1) Subnet Mask
       Parameter Request List Item: (3) Router
       Parameter Request List Item: (6) Domain Name Server
       Parameter Request List Item: (15) Domain Name
       Parameter Request List Item: (31) Perform Router Discover
       Parameter Request List Item: (33) Static Route
       Parameter Request List Item: (43) Vendor-Specific Information
       Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
       Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
       Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
       Parameter Request List Item: (121) Classless Static Route
       Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
       Parameter Request List Item: (252) Private/Proxy autodiscovery
   Option: (82) Agent Information Option
       Length: 20
       Option 82 Suboption: (1) Agent Circuit ID
           Length: 6
           Agent Circuit ID: 00040bb80607
       Option 82 Suboption: (2) Agent Remote ID
           Length: 10
           Agent Remote ID: 030800100201c0a80106
   Option: (255) End
       Option End: 255

No.  Time                 Delta Time     Source             Destination        Protocol
4    18:57:37.184809000   0.000862000    192.168.103.2      192.168.101.1      DHCP

Length    Info
```

```
369       DHCP ACK - Transaction ID 0xae99c7b2

Frame 4: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface 0
Ethernet II, Src: Vmware_96:6d:f7 (00:50:56:96:6d:f7), Dst: 00:38:df:5d:dc:5a (00:38:df:5d:dc:5a)
Internet Protocol Version 4, Src: 192.168.103.2 (192.168.103.2), Dst: 192.168.101.1 (192.168.101.1)
User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)
Bootstrap Protocol (ACK)
   Message type: Boot Reply (2)
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0xae99c7b2
   Seconds elapsed: 0
   Bootp flags: 0x8000 (Broadcast)
       1... .... .... .... = Broadcast flag: Broadcast
       .000 0000 0000 0000 = Reserved flags: 0x0000
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 192.168.101.45 (192.168.101.45)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 192.168.101.1 (192.168.101.1)
   Client MAC address: Vmware_de:32:40 (00:0c:29:de:32:40)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
   Option: (53) DHCP Message Type (ACK)
       Length: 1
       DHCP: ACK (5)
   Option: (58) Renewal Time Value
       Length: 4
       Renewal Time Value: (345600s) 4 days
   Option: (59) Rebinding Time Value
       Length: 4
       Rebinding Time Value: (604800s) 7 days
   Option: (51) IP Address Lease Time
       Length: 4
       IP Address Lease Time: (691200s) 8 days
   Option: (54) DHCP Server Identifier
       Length: 4
       DHCP Server Identifier: 192.168.103.2 (192.168.103.2)
   Option: (1) Subnet Mask
       Length: 4
       Subnet Mask: 255.255.255.0 (255.255.255.0)
   Option: (81) Client Fully Qualified Domain Name
       Length: 3
       Flags: 0x00
       0000 .... = Reserved flags: 0x00
       .... 0... = Server DDNS: Some server updates
       .... .0.. = Encoding: ASCII encoding
       .... ..0. = Server overrides: No override
       .... ...0 = Server: Client
       A-RR result: 255
       PTR-RR result: 255
   Option: (3) Router
       Length: 4
       Router: 192.168.101.1 (192.168.101.1)
   Option: (6) Domain Name Server
       Length: 4
       Domain Name Server: 171.70.168.183 (171.70.168.183)
   Option: (15) Domain Name
       Length: 12
       Domain Name: fabric1.com
   Option: (82) Agent Information Option
       Length: 20
```

```
      Option 82 Suboption: (1) Agent Circuit ID
          Length: 6
          Agent Circuit ID: 00040bb80607
      Option 82 Suboption: (2) Agent Remote ID
          Length: 10
         Agent Remote ID: 030800100201c0a80106
  Option: (255) End
      Option End: 255
```

Debug DHCP

Use the **debug** command if the DHCP binding does not exist.

- The fabric edge receives a DHCP discovery from a DHCP client.
- The DHCP server receives a relayed DHCP discovery/request from the fabric edge (in the default VRF).
- The DHCP server sends a DCHP offer/ack to the fabric edge (in the VRF campus guest).

```
FE1# debug ip dhcp snooping {event | packet}   <-- Assuming that dhcp snooping was enabled via Cisco DNA Center.
 See the preceding configuration.
```

Example output of the debug ip dhcp snooping packet:

```
Jul 26 11:51:55.739: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet2/0/47)
Jul 26 11:51:55.740: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface:
Gi2/0/47, MAC da: ffff.ffff.ffff, MAC sa: 0050.56b4.888b, 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: 0050.56b4.888b, efp_id:
 -517228916, vlan_id: 3000
Jul 26 11:51:55.741: DHCP_SNOOPING: add relay information option.
Jul 26 11:51:55.741: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
Jul 26 11:51:55.741: VRF id is valid
Jul 26 11:51:55.741: LISP ID is valid, encoding RID in srloc format
Jul 26 11:51:55.741: DHCP_SNOOPING: binary dump of relay info option, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F 0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:55.743: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to
 ingress VLAN: (3000)
Jul 26 11:51:55.743: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan3000.
Jul 26 11:51:56.757: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan3000)
Jul 26 11:51:56.758: No rate limit check because pak is routed by this box

Jul 26 11:51:56.758: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Vl3000,
 MAC da: 0050.56b4.888b, MAC sa: 0000.0c9f.fc17, IP da: 172.16.101.3, IP sa: 172.16.101.254, DHCP ciaddr:
0.0.0.0, DHCP yiaddr: 172.16.101.3, DHCP siaddr: 0.0.0.0, DHCP giaddr: 172.16.101.254, DHCP chaddr:
0050.56b4.888b, efp_id: -517228916, vlan_id: 3000
Jul 26 11:51:56.758: DHCP_SNOOPING: binary dump of option 82, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F 0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:56.760: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F
Jul 26 11:51:56.760: DHCP_SNOOPING: binary dump of extracted remote id, length: 12 data:
0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:56.761: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong format or
 not inserted by local switch
Jul 26 11:51:56.761: platform lookup dest vlan for input_if: Vlan3000, is NOT tunnel, if_output: Vlan3000,
if_output->vlan_id: 3000, pak->vlan_id: 3000
Jul 26 11:51:56.762: DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet2/0/47.
Jul 26 11:51:56.763: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet2/0/47)
Jul 26 11:51:56.763: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input interface:
Gi2/0/47, MAC da: ffff.ffff.ffff, MAC sa: 0050.56b4.888b, 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: 0050.56b4.888b, efp_id:
 -517228916, vlan_id: 3000
Jul 26 11:51:56.764: DHCP_SNOOPING: add relay information option.
```

```
Jul 26 11:51:56.764: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
Jul 26 11:51:56.764: VRF id is valid
Jul 26 11:51:56.764: LISP ID is valid, encoding RID in srloc format
Jul 26 11:51:56.764: DHCP_SNOOPING: binary dump of relay info option, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F 0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:56.767: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to
 ingress VLAN: (3000)
Jul 26 11:51:56.767: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan3000.
Jul 26 11:51:56.781: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan3000)
Jul 26 11:51:56.781: No rate limit check because pak is routed by this box

Jul 26 11:51:56.782: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Vl3000,
MAC da: 0050.56b4.888b, MAC sa: 0000.0c9f.fc17, IP da: 172.16.101.3, IP sa: 172.16.101.254, DHCP ciaddr: 0.0.0.0,
 DHCP yiaddr: 172.16.101.3, DHCP siaddr: 0.0.0.0, DHCP giaddr: 172.16.101.254, DHCP chaddr: 0050.56b4.888b,
efp_id: -517228916, vlan_id: 3000
Jul 26 11:51:56.782: DHCP_SNOOPING: binary dump of option 82, length: 22 data:
0x52 0x14 0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F 0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:56.784: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0xB 0xB8 0x2 0x2F
Jul 26 11:51:56.784: DHCP_SNOOPING: binary dump of extracted remote id, length: 12 data:
0x2 0xA 0x3 0x8 0x0 0x10 0x2 0x1 0xC0 0xA8 0x78 0x2
Jul 26 11:51:56.784: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong format or
 not inserted by local switch
Jul 26 11:51:56.785: DHCP_SNOOPING: add binding on port GigabitEthernet2/0/47 ckt_id 0 GigabitEthernet2/0/47
Jul 26 11:51:56.785: DHCP_SNOOPING: added entry to table (index 245)

Jul 26 11:51:56.785: DHCP_SNOOPING: dump binding entry: Mac=00:50:56:B4:88:8B Ip=172.16.101.3 Lease=600
Type=dhcp-snooping Vlan=3000 If=GigabitEthernet2/0/47
Jul 26 11:51:56.785: No entry found for mac(0050.56b4.888b) vlan(3000) GigabitEthernet2/0/47
Jul 26 11:51:56.785: host tracking not found for update add dynamic (172.16.101.3, 0.0.0.0, 0050.56b4.888b)
vlan(3000)
Jul 26 11:51:56.785: platform lookup dest vlan for input_if: Vlan3000, is NOT tunnel, if_output: Vlan3000,
if_output->vlan_id: 3000, pak->vlan_id: 3000
Jul 26 11:51:56.786: DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet2/0/47.
```

Note As you can see in this example, a lot of messages can be displayed in the console when logging is enabled. To disable the display of these messages, run the **no logging console** command.

Capture Packets Using Embedded Wireshark

Wireshark is supported on some Cisco Catalyst switches. For more information, see Configuring Wireshark. Complete the following steps to capture incoming UDP packets.

Procedure

Step 1 Configure a new monitor capture.

```
c3850-edge2#monitor capture test interface GigabitEthernet 2/0/1 in match ipv4 protocol udp any any

c3850-edge2#show monitor capture

Status Information for Capture test
  Target Type:
 Interface: GigabitEthernet2/0/1, Direction: IN
   Status : Inactive
```

```
  Filter Details:
   IPv4
    Source IP: any
    Destination IP: any
   Protocol: udp
 Buffer Details:
  Buffer Type: LINEAR (default)
 File Details:
  File not associated
 Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 0 (no limit)
  Packet Size to capture: 0 (no limit)
  Packet sampling rate: 0 (no sampling)
```

Step 2 Start a monitor capture.

```
c3850-edge2#monitor capture test start
Started capture point : test
c3850-edge2#
Jul 26 11:51:43.087: %BUFCAP-6-ENABLE: Capture Point test enabled.
```

```
c3850-edge2#show monitor capture

Status Information for Capture test
  Target Type:
 Interface: GigabitEthernet2/0/1, Direction: IN
   Status : Active
  Filter Details:
   IPv4
    Source IP: any
    Destination IP: any
   Protocol: udp
 Buffer Details:
  Buffer Type: LINEAR (default)
  Buffer Size (in MB): 10
 File Details:
  File not associated
 Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 0 (no limit)
  Packet Size to capture: 0 (no limit)
  Maximum number of packets to capture per second: 1000
  Packet sampling rate: 0 (no sampling)
```

Step 3 Stop a monitor capture.

```
c3850-edge2#monitor capture test stop
Capture statistics collected at software:
        Capture duration - 25 seconds
        Packets received - 5
        Packets dropped - 0
        Packets oversized - 0

Packets dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : test
c3850-edge2#
Jul 26 11:52:08.754: %BUFCAP-6-DISABLE: Capture Point test disabled.
```

```
c3850-edge2#show monitor capture

Status Information for Capture test
```

```
 Target Type:
Interface: GigabitEthernet2/0/1, Direction: IN
  Status : Inactive
 Filter Details:
  IPv4
   Source IP: any
   Destination IP: any
  Protocol: udp
Buffer Details:
 Buffer Type: LINEAR (default)
 Buffer Size (in MB): 10
File Details:
 File not associated
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Maximum number of packets to capture per second: 1000
 Packet sampling rate: 0 (no sampling)
```

Step 4 Show a captured packet. Use **show monitor capture test buffer** to decode the captured packets in detail.

```
c3850-edge2#show monitor capture test buffer
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000  192.168.1.1 -> 192.168.120.2 UDP 112 Source port: 65414 Destination port: vxlan
  2   0.000032  192.168.1.1 -> 192.168.120.2 UDP 400 Source port: 54163 Destination port: vxlan
  3   0.000055  192.168.1.1 -> 192.168.120.2 UDP 400 Source port: 54164 Destination port: vxlan
  4   0.000077 192.168.99.11 -> 192.168.120.2 RADIUS 558 Access-Accept(2) (id=113, l=516)
  5   0.000099 192.168.99.11 -> 192.168.120.2 RADIUS 313 Access-Accept(2) (id=114, l=271)
```

Step 5 Export the packet to a .pcap file.

```
c3850-edge2#monitor capture test export location flash:test.pcap
Export Started Successfully
```

```
c3850-edge2#copy flash:test.pcap tftp://10.70.69.134/taisasak/test.pcap vrf Mgmt-vrf
Address or name of remote host [10.70.69.134]?
Destination filename [taisasak/test.pcap]?
!!
2152 bytes copied in 0.024 secs (89667 bytes/sec)
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.