Troubleshoot APIPA Address Failure in the Network

Contents

Introduction

Components used

Reasons

Scenarios & Troubleshooting

- Scenario 1 -Firewall proxy configuration
  - Problem description:
  - Problem symptoms
  - Troubleshooting steps
  - Isolation
  - Plan of action
  - Resolution/Verification
- Scenario 2 -DHCP server scope
  - Problem description:
  - Symptoms
  - Troubleshooting performed
  - Isolation
  - Plan of action
  - Resolution/Verification
- Scenario 3 -C9300 SDA configuration
  - Problem description:
  - User symptoms
  - Troubleshooting performed
  - Isolation
  - Plan of action
  - Resolution/Verification
- Scenario 4 -LAN Adaptor problem
  - Problem description:
  - Symptoms
  - Troubleshooting steps
  - Isolation
  - Plan of action
  - Resolution/Verification
- Scenario 5 -MTU Mismatch
  - Problem description:
  - User symptoms
  - Troubleshooting performed
  - Isolation
  - Plan of action
  - Resolution/Verification
- Scenario 6 - IPDT Guard
  - Problem description:
  - User symptoms
  - Troubleshooting performed

Isolation
Plan of action
Resolution/Verification

Introduction

This document describes the issues related to APIPA addresses and provides resolutions for the same.

Components used

- Catalyst 9000 switches.
- ASA Firewalls like 5516
- DHCP server of any kind
- Catalyst 9300 in SDA setup
- Software: N/A

Reasons

End users assign APIPA during these scenarios,

- DHCP server not available.
- DHCP Offer is dropped before or current hop.
- ARP probe gets a response which represents Duplicate IP.

Scenarios & Troubleshooting

Scenario 1 - Firewall proxy configuration



ASA 5516

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

Problem symptoms

1. Users on a specific VLAN experience intermittent issues where they receive an APIPA IP address and lose connectivity to the network.
2. Firewalls have multiple ARP entries for a single end user MAC address like this:

<#root>

```
Firewall/pri/act# show arp | include abcd.abcd.abcd
```

```
inside 10.1.1.12 abcd.abcd.abcd 30

inside 10.1.1.13 abcd.abcd.abcd 40

inside 10.1.1.14 abcd.abcd.abcd 51

inside 10.1.1.15 abcd.abcd.abcd 53
```

Troubleshooting steps

1. Debugs on Firewall points to the firewall sending the response to end users ARP probe.

<#root>

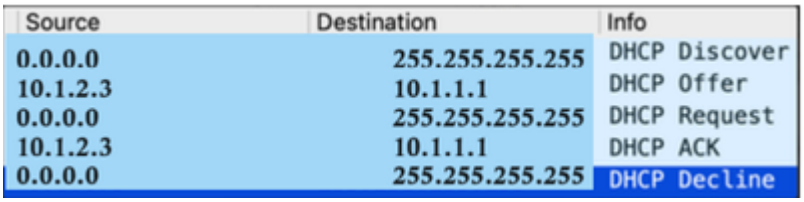
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).

DHCPRA: Adding rule to allow client to respond using offered address 10.1.1.12
```

This makes the end device to think its a duplicate address.

2. Captures on end device or Firewall

Captures show end device sending DHCP Decline packets once DORA process gets completed.



Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Isolation

- Firewall inside interface responds to the ARP probe by acting as proxy, once the DORA process is completed. This makes the PC to send DHCP decline.

Plan of action

- Disable the proxy arp on Firewall inside interface using the command "sysopt noproxyarp inside"

Resolution/Verification

- End devices receive IP address after disabling proxy-arp.
- **Note: Make sure no device acts as proxy or sends response for end user ARP probes.**

.

Scenario 2 - DHCP server scope



DHCP Server

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

Symptoms

1. Users on specific vlan gets only APIPA IP address and lose connection to network.

Troubleshooting performed

- DHCP decline sent to end users and it was configured with APIPA address

Isolation

- DHCP server assigns one ip address from scope A and same ip address being assigned to another Laptop because scope B has same range. This causes DHCP decline:
-

Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Plan of action

- Assign unique DHCP scope range

Resolution/Verification

- End devices receive IP address after scope change.
- **Note: Make sure DHCP server does not have duplicate scopes configured.**

Scenario 3 -C9300 SDA configuration



Cat9300 in SDA

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

User symptoms

1. Some users in a specific VLAN are not able to obtain DHCP addresses through the wireless AP.
2. Firewall had multiple arp entries for a single end user mac address

<#root>

```
Firewall# show arp | i abcd


Inside 10.1.1.22 abcd.abcd.abcd 48


Inside 10.1.1.23 abcd.abcd.abcd 49


Inside 10.1.1.24 abcd.abcd.abcd 50
```

Troubleshooting performed

- DHCP Offer was dropped by switch
- FTD populate ARP based on DHCP OFFER coming back from DHCP server.

<#root>

```
***DROP*** Broadcast to Access-Tunnel disallowed (accessTunnelBroadcastDrop)
```

Isolation

- If L2-only VLAN is configured for SDA wireless setup, offer packet with broadcast flag do not reach AP. Since Access-tunnel doesn’t allow broadcast packets by default.

Plan of action

- Allow "flood capability" inside LISP environment.

<#root>

```
router lisp


instance-id 8456


flood access-tunnel
```

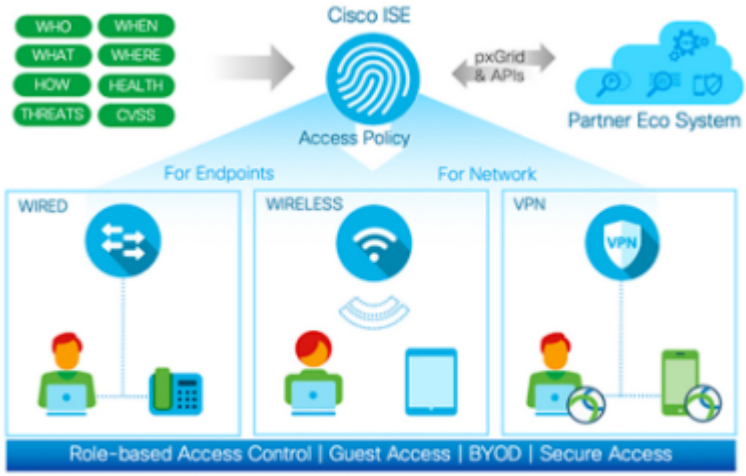
Resolution/Verification

- After configuring `flood access-tunnel` in the C9300 connected on inside interface, clients receive DHCP addresses.



Note: Make sure to enable flood access-tunnel under lisp, if end device is configured to receive broadcast offer.

Scenario 4 - LAN Adaptor problem



cisco ISE

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

Symptoms

1. Mac address-table shows entries with "drop".

<#root>

```
#show mac address-table interface gigabitethernet1/0/20


Mac Address Table


-------------------------------------------


Vlan    Mac Address       Type        Ports


----    -----------       --------    -----


10    0000.0001.000a    DYNAMIC     Drop
```

2. The Show Authentication session shows many entries, possibly exceeding 2000 or even 10000.

<#root>

```
switch2#show authentication sessions


Gi1/0/1  0000.0001.1234 N/A   UNKNOWN Unauth  0AFF0B8D000000EC000000AF


Gi1/0/1  0000.0001.2345 N/A   UNKNOWN Unauth  0AFF0B8D000000F00016B7D7


Gi1/0/1  0000.0001.3456 N/A   UNKNOWN Unauth  0AFF0B8D0028DE3500000000
```

Troubleshooting steps

- Packet capture shows many incoming packets from end device with different Source MAC addresses.
- The Auth session limit is 2000 and once the limit is crossed unexpected issues arise in network
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-12/configuration_guide/sec/b_1612_sec_3650_cg/configuring_ieee_802_1x_port_based_authentication.html

Isolation

- This is an indication of end user Adaptor problem.This sends malformed packets which the switch understands as Random source mac addresses.

Plan of action

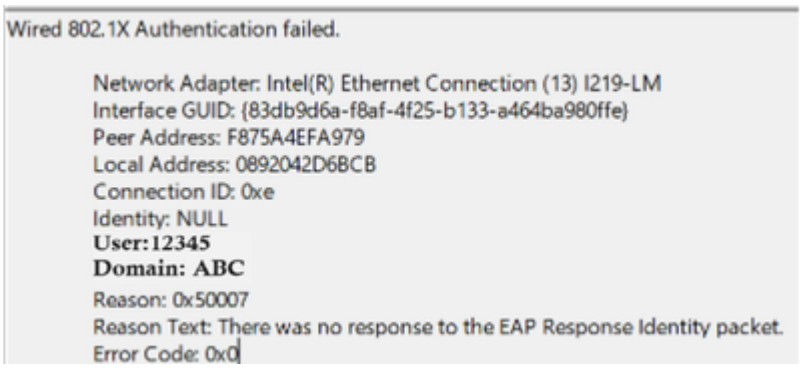
- Configure "authentication host-mode multi-domain" which allows only 2 mac addresses.
- Identify and isolate the culprit device.

Resolution/Verification

- After configuring this workaround no issue be observed.

- **Note**: Make sure to enable either port-security or Dot1x auth session host-mode multi-domain.

Scenario 5 - MTU Mismatch



ISE represents this error on the server.

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

User symptoms

1. End client sends EAP response with packet length higher than (Example: 3736) the actual expected packet length 1492.

```
Extensible Authentication Protocol
Code: Response (2)
Id: 4
Length: 1492
Type: TLS EAP (EAP-TLS) (13)
· EAP-TLS Flags: 0xc0
..0. .... = Start: False
EAP-TLS Length: 3736
```

Troubleshooting performed

- MTU set to less size on switch as a system wide entry. (Example:1998bytes)
- Egress interface configured with higher size. (Example: 9198bytes)

Isolation

- Mismatch in MTU throughout the path cause the problem.

Plan of action

- Change the system MTU to 1500 and Reload the switch

Resolution/Verification

- After configuring this settings, the authentication becomes successful.
- **Note**: Make sure to enable same MTU throughout the path of packet flow.

Scenario 6 - IPDT Guard

Problem description:

- User machines recieve APIPA IP address and user connectivity impacted.

User symptoms

- When having VMs in HA, if you have this policy applied in the interface:

device-tracking policy IPDT_POLICY

no protocol udp

tracking enable

- After a failover, ARP reply gets dropped by the access switch.

Troubleshooting performed

1. ARP responses to the probes would be getting dropped by switch.
2. Switch is configured with IPDT Guard.
3. IPDT - Guard dropping ARP probe & end device getting APIPA.

Isolation

- ARP probe packets reaching IPDT and gets dropped due to the Guard feature.
- IPDT policy configured with 'security-level guard' config drops ARP packets causing few or all end devices to be unreachable

Plan of action

- Change the setting from Guard to Glean.
  Configure 'security-level glean' in the IPDT policy

Resolution/Verification

- After configuring glean settings the ARP probes get processed by the ARP process & Issue gets resolved.
-

Note: This is a well known defect and it would be fixed in 17.15.1 version and later.