Cisco DNS-AS Troubleshooting

First Published: May 11, 2016
Last Updated: May 17, 2016

Contents

Introduction

This guide addresses client-side troubleshooting for Cisco DNS-AS.

About DNS-AS

Working together with Cisco NBAR2, "DNS as Authoritative Source," DNS-AS, provides centralized control of custom application classification information. Classification information (metadata such as application name, ID, traffic class, business relevance, and so on) is used by NBAR2 to recognize the network traffic of specific applications, and to classify the traffic by assigning parameters useful both in reporting and in applying network traffic policy.

DNS-AS feature includes configuration and functionality on:

- One or more routers (clients) in a network
- One more DNS-AS servers that communicate with the clients

Verifying Configuration Changes

After making changes to the DNS-AS configuration on client or server, verify the changes using the show commands described in the “Monitoring DNS-AS” section of DNS-AS in the NBAR Configuration Guide. Test DNS-AS functionality by generating traffic for the applications configured with the feature, then use the show commands to confirm that the binding table has been created correctly on the routers operating with DNS-AS.

When Is Troubleshooting Necessary

Any of the following may suggest client-side problems with DNS-AS:

- If... Custom protocols are not being created by DNS-AS on the client router.
- If... Network operations, such as traffic reporting, that depend on customized application handling through the DNS-AS feature are not functioning as expected.

How to Use this Guide

This guide provides DNS-AS Troubleshooting Tools that you can use individually, a Comprehensive Troubleshooting Workflow, and specific Problem Scenarios with recommended troubleshooting steps.

DNS-AS Troubleshooting Tools

Use the diagnostic tools described in this section individually or as part of a troubleshooting workflow, such as the Comprehensive Troubleshooting Workflow.

Diagnostic Tool: Verify Customization Interval

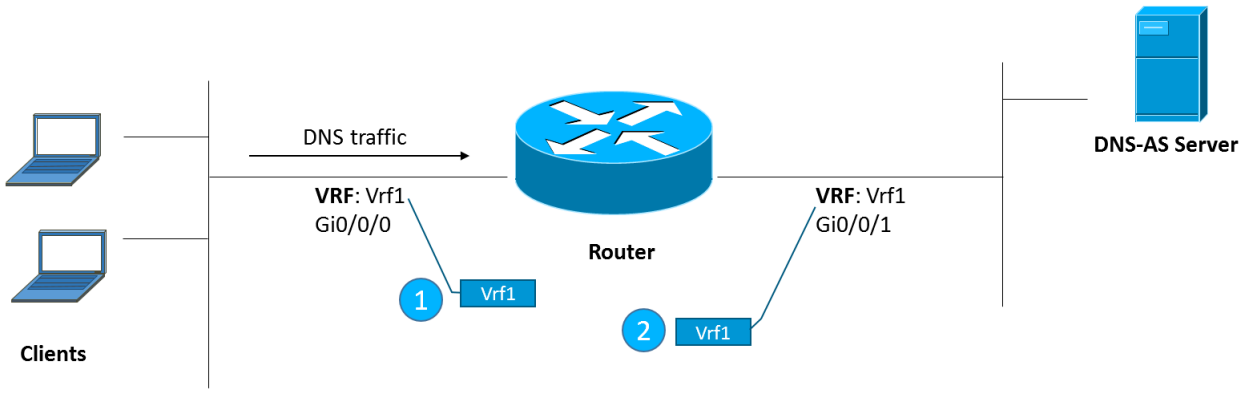
The DNS-AS binding table is regenerated on the router every 5 minutes, by default. This is the "customization interval," the time during which the router collects auto-learn raw data before creating new custom protocols (see Showing the DNS-AS custom-application Data in the NBAR Configuration Guide).

Verify that the traffic has been run on the router. The traffic may not lead to the creation of new custom protocols in the binding table for a period of 5 minutes.

Diagnostic Tool: Verify that Traffic Interface and DNS-AS Server on Same VRF

The DNS query traffic and the DNS-AS server must be on the same VRF.

Figure 1. Verifying that Traffic Interface and DNS-AS Server on the Same VRF



Use show ip vrf to verify that the traffic interface and the interface connected to the DNS-AS server are assigned to the same VRF.

```
router#show ip vrf
  Name              Default RD            Interfaces
  Vrf1              <not set>             Gi0/0/0
                                          Gi0/0/1
```

Diagnostic Tool: Verify that DNS-AS Server Is Specified on DNS-AS Client Device

Use show avc dns-as client name-server brief to verify that the correct DNS-AS server IP address is configured on the DNS-AS client device. In this example, the DNS-AS server address is 1.1.1.1.

```
router#show avc dns-as client name-server brief

 Server-IP                | Vrf-name
-------------------------------------------------------
 1.1.1.1                   | vrf1
```

Diagnostic Tool: Check Connectivity between DNS-AS Client Device and DNS-AS Server

Use ping to check the connectivity from the DNS-AS client device to the DNS-AS server.

ping <*vrf*> <*dns-as-server ip*>

In this example, the ping results confirm connectivity.

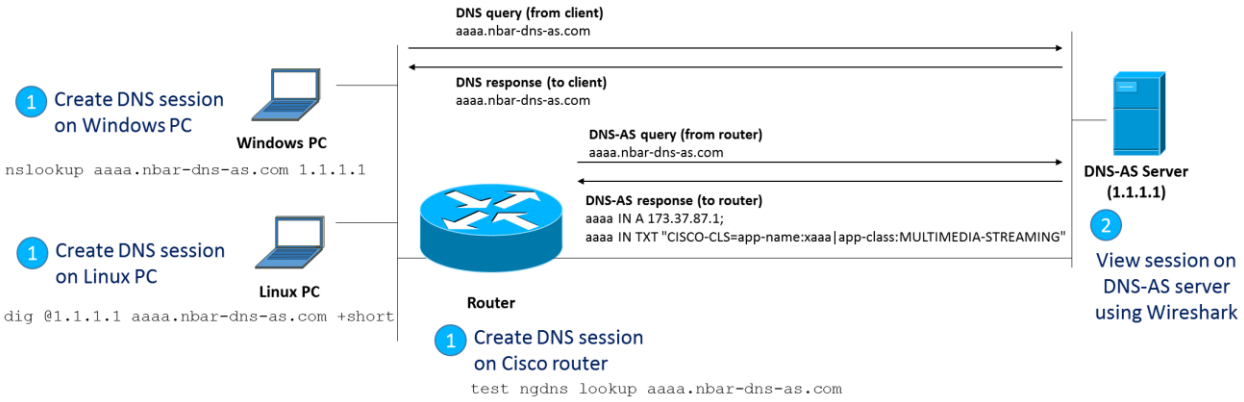
```
router#ping vrf vrf1 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Diagnostic Tool: DNS Session Simulation

To simulate a DNS session between the DSN-AS client (router) and the DNS-AS server, send DNS queries (A and TXT) from the router to the DNS-AS server and examine the DNS records configured on the server.

1. Use one of the following options to create DNS query traffic:
   - DNS Session Option A: Generate DNS Traffic Using Cisco Router DNS-AS Client
   - DNS Session Option B: Generate DNS Traffic Using Windows PC
   - DNS Session Option C: Generate DNS Traffic Using Linux PC
2. After generating the DNS requests, view the DNS session information. See Diagnostic Tool: View DNS Session Using Wireshark.

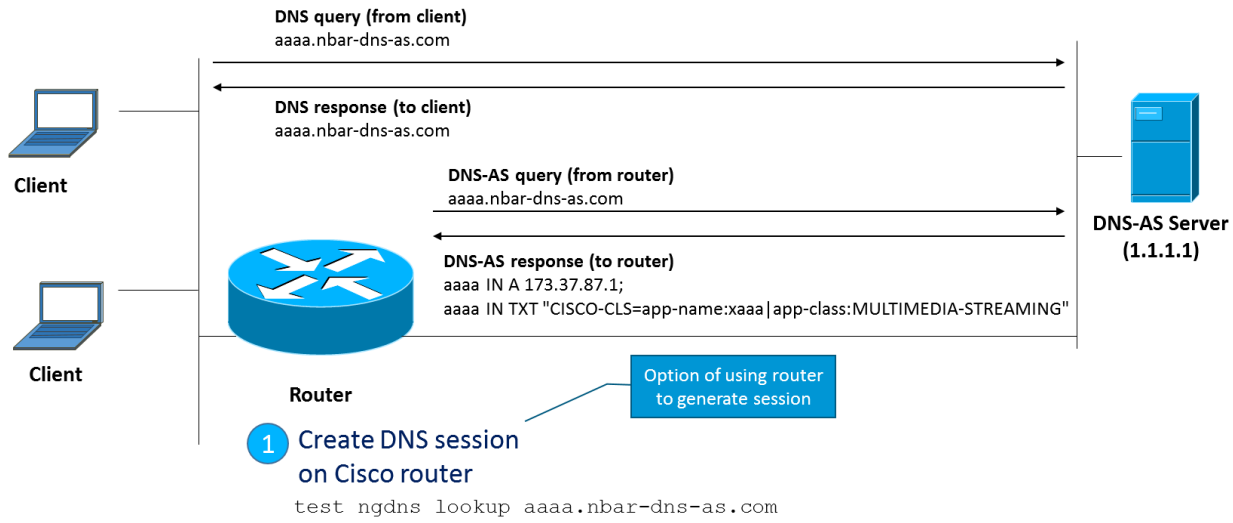
Figure 2. Overview of DNS Session Simulation: Create traffic, then View Session



DNS Session Option A: Generate DNS Traffic Using Cisco Router DNS-AS Client

This procedure specifies a DNS-AS server and generates DNS query traffic to the server.

Figure 3. Generating DNS Traffic Using a Cisco Router



1. On the DNS-AS client (Cisco router), check the address of the configured DNS-AS server. Use one of the following commands:

   - (Not using VRF) ip name-server <*server-ip*>
   - (Using VRF) ip name-server vrf <*vrf-name*> <*dns-as-server ip*>

2. In global configuration mode, execute the service internal troubleshooting command to enable test commands used in the troubleshooting steps in this section.

Note: This command is used in advanced troubleshooting. After completing the troubleshooting, disable the feature using the no service internal command.

```
Router#conf t
Router(config)#service internal
```

3. (Optional) Set the configuration parameters for generating the DNS request.

   test ngdns config vrf <*vrf-name*>

4. Generate a DNS A query.

test ngdns <*domain-name*>

5. Generate a DNS TXT query.

test ngdns <*domain-name*> type txt

6. Display the router host table. Use one of the following commands:

   - (Not using VRF) show hosts
   - (Using VRF) show hosts vrf <*vrf-name*>

Example

In this example:

- A DNS query for the “aaaa.nbar-dns-as.com” domain is sent to a DNS-AS server.
- Router is using VRF
- The server IP address is 1.1.1.1

The initial steps generate the DNS requests.

```
router#conf t
Router(config)#service internal
Router#test ngdns config vrf Mgt
Router#test ngdns lookup aaaa.nbar-dns-as.com
 DNS result:
        173.37.87.1
        Result is insecure
        flags = 0x0
        extended flags = 0x0
synchronous resolve done successfully
Finished resolving in 0.007 seconds.
```

```
router#test ngdns lookup aaaa.nbar-dns-as.com  type txt
ISR4431-Matrix#DNS result:
        "CISCO-CLS=app-name:aaaa|app-class:MULTIMEDIA-STREAMING"
        Result is insecure
        flags = 0x0
        extended flags = 0x0
synchronous resolve done successfully
Finished resolving in 0.003 seconds.
```

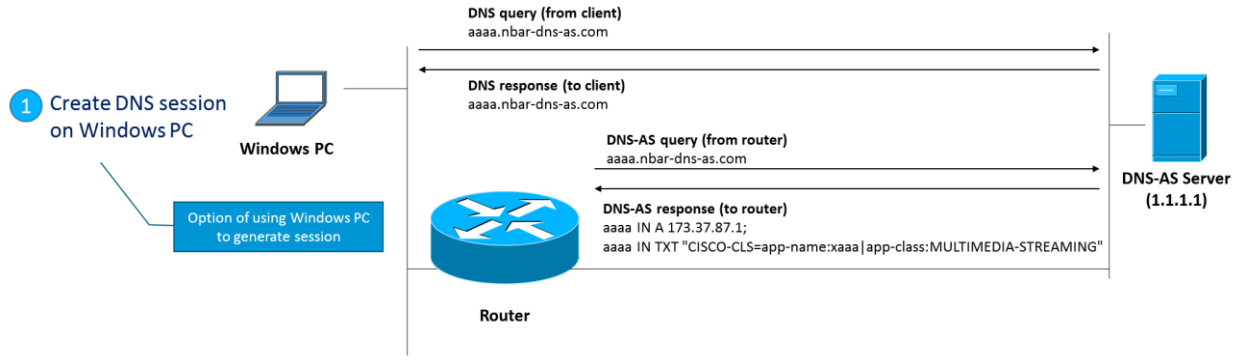
The final step displays the router's host table, showing the information provided by DNS-AS in the TXT response, and the address for the requested domain in the A response (shown in bold).

```
router#show hosts vrf Mgt
Name lookup VRF: Mgt
Default domain is not set
Name servers are 1.1.1.1
NAME   TTL   CLASS    TYPE       DATA/ADDRESS
-----------------------------------------

aaaa.nbar-dns-as.com    85791    IN       TXT      "CISCO-CLS=app-name:aaaa|app-class:MULTIMEDIA-STREAMING"
aaaa.nbar-dns-as.com    85777    IN       A        173.37.87.1
```

DNS Session Option B: Generate DNS Traffic Using Windows PC

This procedure generates DNS query using a Windows PC in the network.

Figure 4. Generating DNS Traffic Using Windows PC



1. On the Windows PC, open a command line window and use the nslookup command to generate a DNS A session.

   nslookup <*domain*> <*dns-server ip*>

2. Use nslookup as follows to generate a DNS TXT session.

   nslookup -type=txt <*domain*> <*dns-server ip*>

Example

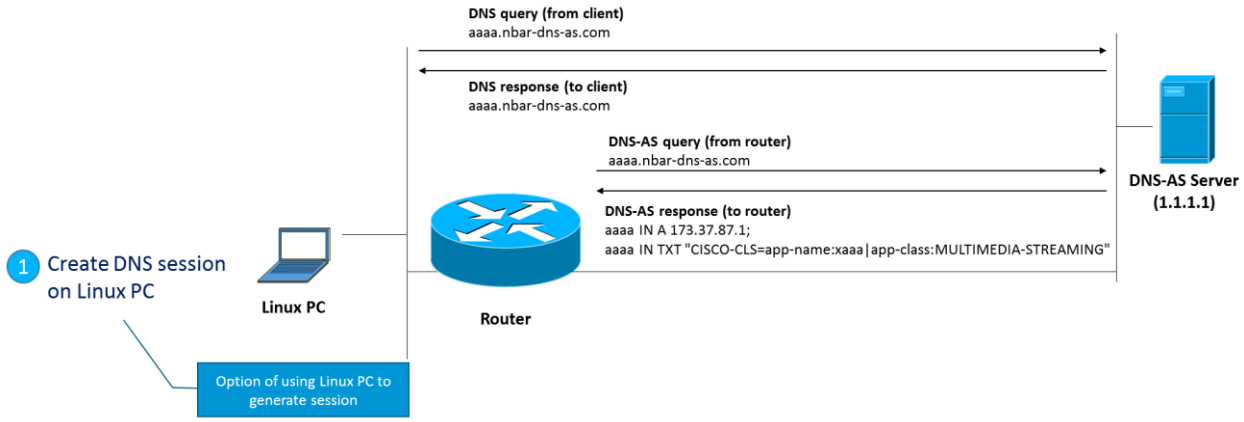
In this example, nslookup creates DNS A and TXT queries for aaaa.nbar-dns-as.com.

```
C:>nslookup aaaa.nbar-dns-as.com 10.56.196.51
Server: UnKnown
Address: 10.56.196.51

Name: aaaa.nbar-dns-as.com
Address: 20.0.0.2

C:>nslookup -type=TXT aaaa.nbar-dns-as.com 10.56.196.51
Server: UnKnown
Address: 10.56.196.51

aaaa.nbar-dns-as.com    text =

     "CISCO-CLS=app-name:aaaa|app-class:MULTIMEDIA-STREAMING"
nbar-dns-as.com nameserver = ns1.dns-lab.com
C:>
```

DNS Session Option C: Generate DNS Traffic Using Linux PC

This procedure generates DNS query using a client Linux PC in the network.

Figure 5. Generating DNS Traffic Using Linux PC



1. On the Linux PC, at a command line interface, use the dig command to generate a DNS query.

   dig @<*server-ip*> <*domain*> +short

2. Use the dig command as follows to generate a TXT query.

   dig txt @<*server-ip*> <*domain*> +short

Example

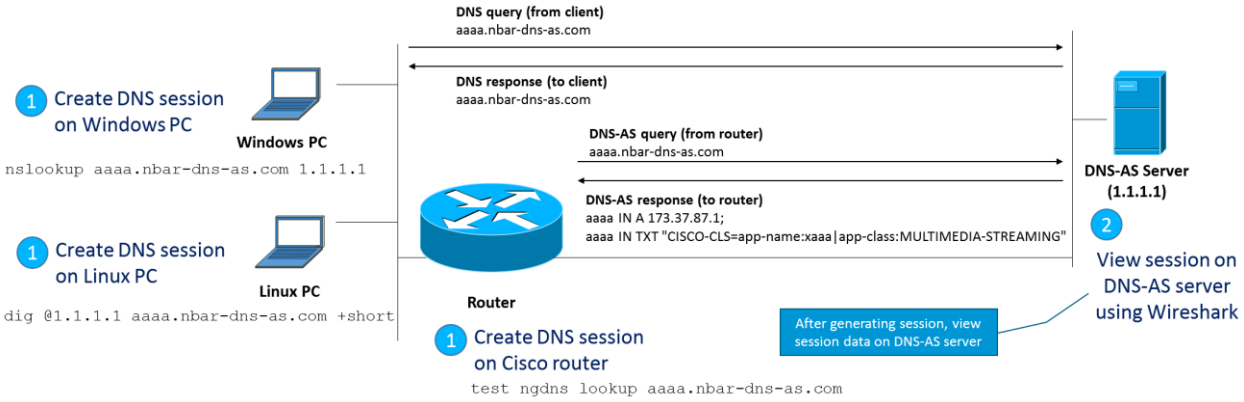
In this example, dig creates DNS A and TXT queries for aaaa.nbar-dns-as.com.

```
linux>dig @10.56.128.34 xaaa.server.world +short
                      173.37.87.1

linux>dig txt @10.56.128.34 xaaa.server.world +short
"CISCO-CLS=app-name:xaaa|app-class:MULTIMEDIA-STREAMING"
```

Diagnostic Tool: View DNS Session Using Wireshark

On the DNS-AS server, use a packet analyzer application, such as the popular Wireshark, to view the DNS session data.

Figure 6. Viewing DNS Session Using Wireshark



Diagnostic Tool: Check the DNS-AS Client Statistics

On the DNS-AS client (router), use the show avc dns-as client statistics command to display the DNS-AS client statistics. The command output shows whether the DNS-AS client sent queries to the DNS-AS server, and shows whether the server responded.

In the show avc dns-as client statistics output, check the “TXT Query TX packets” (shown in bold). A value of 0 indicates that the DNS-AS client (router) has not sent any queries to the server.

Example 1: No DNS queries sent, no responses received

This example output shows a value of 0 for “TXT Query TX packets”.

```
router#show avc dns-as client statistics
Server details: vrf-id = 2 vrf-name = vrf1 ip = 1.1.1.1
 AAAA  Query    Error packets    0
 AAAA  Query    TX    packets      0
 AAAA  Response RX    packets   0
     TXT  Query    Error packets     0
     TXT  Query    TX    packets      0
     TXT  Response RX    packets   0
         A  Query    Error packets     0
         A  Query    TX    packets       0
         A  Response RX    packets   0
```

Example 2: DNS queries sent, responses received

This more typical example output shows correct functionality. The router has sent several DNS queries to the server. The query and response packet counts should be equal.

```
router#show avc dns-as client statistics
Server details: vrf-id = 2 vrf-name = vrf1 ip = 1.1.1.1
 AAAA  Query       Error packets 0
 AAAA  Query       TX      packets 100
 AAAA  Response RX     packets 100
     TXT  Query    Error    packets 0
     TXT  Query    TX        packets  300
     TXT  Response RX     packets 300
           A  Query    Error  packets 0
           A  Query    TX       packets 200
           A  Response RX     packets 200
```

Diagnostic Tool: Check for Pending Queries

The DNS-AS client caches incoming DNS queries for an interval (default: 3 minutes) before sending queries to the DNS-AS server. During this time, they are called “pending” queries.

If the show avc dns-as client statistics output indicates that no DNS queries have been sent to the server, the reason could be that the queries are still pending.

Use the ip nbar classification auto-learn dns-as-client pending-queries command to check for pending queries.

Example 1: No Pending Queries

This output example shows no pending queries.

```
Router#show ip nbar classification auto-learn dns-as-client pending-queries
AAAA queries pending inject 0
AAAA queries injected            0
 TXT queries pending inject    0
 TXT queries injected               0
   A queries pending inject      0
   A queries injected                 0
```

Example 2: Pending Queries

This output example shows pending queries.

```
Router#show ip nbar classification auto-learn dns-as-client pending-queries
AAAA queries pending inject 0
AAAA queries injected            0
 TXT queries pending inject   300
 TXT queries injected             500
   A queries pending inject     300
   A queries injected               500
```

Diagnostic Tool: Check Trusted Domains Configured on Router

Check the configured trusted domains on the router. The router sends a DNS request to the DNS-AS server only for applications specified as trusted domains. Use show run command, piped to the sec command to display the configured trusted domains.

show run | sec trusted-domains

Example: Trusted domains

```
router#show run | sec trusted-domains
avc dns-as client trusted-domains
 domain *cisco.com
 domain *google.com
```

Diagnostic Tool: Display Information Learned from the DNS-AS Server

The show ip nbar classification auto-learn dns-as-client 100 detailed command displays the application information that a router has received from the DNS-AS server, arranged by domain.

Example: Application data learned from DNS-AS server

In this example, the router has information for 10 applications.

```
Router#show ip nbar classification auto-learn dns-as-client 100 detailed
-------------------------------------------------------------------------------------------------
  #|Host                   |Vrf    |IP List       |Text
-------------------------------------------------------------------------------------------------
  1|hose.nbar-dns-as.com   |Mgt    |2.1.40.207    |app-name:hose|app-class:MULTIMEDIA-STREAMING
  2|hshp.nbar-dns-as.com   |Mgt    |2.1.50.76     |app-name:hshp|app-class:BROADCAST-VIDEO
  3|hsjo.nbar-dns-as.com   |Mgt    |2.1.50.127    |app-name:hsjo|app-class:TRANSACTIONAL-DATA
  4|apxl.nbar-dns-as.com   |Mgt    |20.0.38.235   |app-name:apxl|app-class:REALTIME-INTERACTIVE
  5|annk.nbar-dns-as.com   |Mgt    |20.0.33.14    |app-name:annk|app-class:MULTIMEDIA-STREAMING
  6|hwij.nbar-dns-as.com   |Mgt    |2.1.60.240    |app-name:hwij|app-class:TRANSACTIONAL-DATA
  7|hyjn.nbar-dns-as.com   |Mgt    |2.1.66.86     |app-name:hyjn|app-class:NETWORK-CONTROL
  8|cgfo.nbar-dns-as.com   |Mgt    |40.0.15.51    |app-name:cgfo|app-class:NETWORK-CONTROL
  9|cpsm.nbar-dns-as.com   |Mgt    |40.0.38.111   |app-name:cpsm|app-class:MULTIMEDIA-STREAMING
 10|cbic.nbar-dns-as.com   |Mgt    |40.0.3.61     |app-name:cbic|app-class:BROADCAST-VIDEO
```

Problem Scenarios

DNS-AS client auto-custom binding table is empty

Symptoms

The show avc dns-as client binding-table command displays the auto-custom bind table. The following example shows and empty binding table, indicated by “No data available yet” (bold added).

```
router#show avc dns-as client binding-table
DNS-AS generated protocols:
 Max number of protocols      :50
 Customization interval [min] :5
 No data available yet
```

Troubleshooting Steps

Use the Comprehensive Troubleshooting Workflow.

DNS-AS custom protocols do not appear in the router’s binding table

Symptoms

The results of the show ip nbar protocol-discovery stats packet-count command do not show the custom protocols generated by DNS-AS.

Troubleshooting Steps

Use the Comprehensive Troubleshooting Workflow.

Comprehensive Troubleshooting Workflow

The comprehensive client-side troubleshooting workflow addresses the following common issues affecting DNS-AS function:

Category	Potential Problem	Description
Connectivity	Network connectivity	Connectivity problems between the DNS-AS client (router) and the DNS-AS server. ■ Step 1: Verify connectivity
	Server specification	Wrong DNS-AS server specified on the client device. ■ Step 2: Verify that the client specifies the DNS-AS server correctly
	DNS session	DNS query/response not successful. ■ Step 3: Verify that DNS-AS server replies to queries ■ Step 4: Verify that DNS-AS client queries reach DNS-AS server ■ Step 5: Check for pending queries on the DNS-AS client ■ Step 6: Verify that router has received information from the DNS-AS server
Client (router)	Trusted domain configuration	Wrong DNS-AS trusted-domain configuration on the DNS-AS client device. The trusted domain configuration specifies the applications that are handled by the DNS-AS feature. ■ Step 7: Verify the trusted domains
	Custom protocol creation	Problem with completing the process of custom protocol creation. ■ Step 8: Check the binding table ■ Step 9: Verify custom protocols
DNS-AS server	Server configuration	Incorrect DNS-AS record configuration on the DNS-AS server. ■ Step 10: On the DNS-AS server, verify the TXT records

Step 1: Verify connectivity

Check connectivity between the DNS-AS client (router) and the DNS-AS server.

Procedure

Use the ping <*dns-as-server ip*> command.

See Diagnostic Tool: Check Connectivity between DNS-AS Client Device and DNS-AS Server.

Results

If the server does not respond to the ping, there is a basic connectivity problem between the client and server.

Step 2: Verify that the client specifies the DNS-AS server correctly

Verify that the client (router) is configured correctly to connect to the DNS-AS server.

Procedure

Use the show avc dns-as client name-server brief command to display the configured DNS-AS server(s).

Results

Expected result: One or more correct DNS-AS servers are configured. The server(s) must be accessible, as tested in Step 1: Verify connectivity.

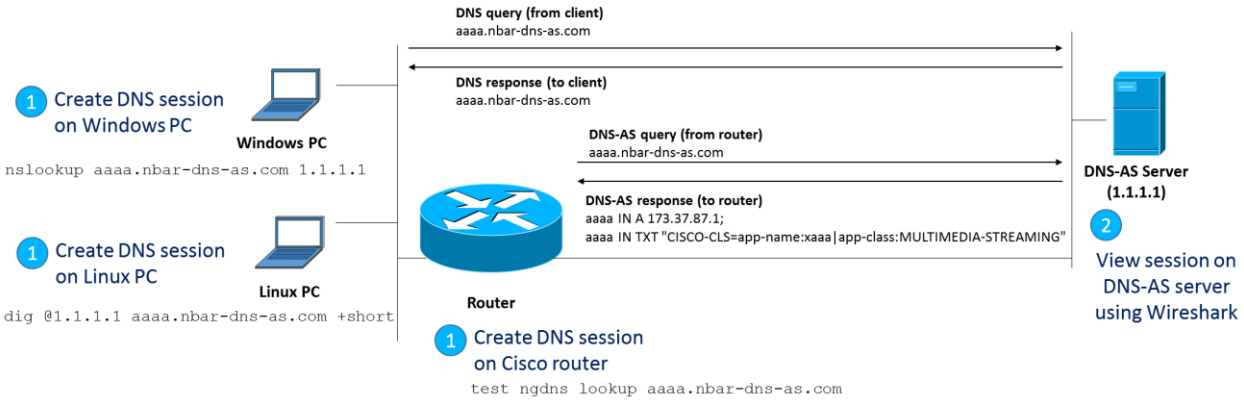
Step 3: Verify that DNS-AS server replies to queries

Verify that the DNS-AS server replies to DNS A and TXT queries from the client (router).

Procedure

1. Use one of the following options to create DNS query traffic:
   - DNS Session Option A: Generate DNS Traffic Using Cisco Router DNS-AS Client
   - DNS Session Option B: Generate DNS Traffic Using Windows PC
   - DNS Session Option C: Generate DNS Traffic Using Linux PC
2. After generating the DNS requests, view the DNS session information. See Diagnostic Tool: View DNS Session Using Wireshark.

Figure 7. Viewing DNS Session Information



Results

Expected result: DNS requests appear in the DNS session information.

Step 4: Verify that DNS-AS client queries reach DNS-AS server

Verify that the DNS-AS client (router) has sent DNS requests to the DNS-AS server, including:

- A (for IPv4 address) or AAAA (for IPv6 address) queries
- TXT queries

Procedure

Use the show avc dns-as client statistics command, described in Diagnostic Tool: Check the DNS-AS Client Statistics.

Results

Expected result: show avc dns-as client statistics output indicates queries sent and responses received. If none are displayed, the reason could be that the router has pending queries that have not yet been sent to the DNS-AS server. See Step 5: Check for pending queries on the DNS-AS client.

Step 5: Check for pending queries on the DNS-AS client

Check for pending queries on the DNS-AS client (router).

The DNS-AS client caches incoming DNS queries for an interval (default: 3 minutes) before sending queries to the DNS-AS server. During this time, they are called “pending” queries.

If the show avc dns-as client statistics output indicates that no DNS queries have been sent to the server, the reason could be that the queries are still pending.

Procedure

Use the ip nbar classification auto-learn dns-as-client pending-queries command to check for pending queries. See .Diagnostic Tool: Check for Pending Queries.

Results

Expected result: Counters increase after each inject interval (3 minutes). If the results do not show this, determine why no DNS requests are being made.

Step 6: Verify that router has received information from the DNS-AS server

Verify that the DNS-AS client (router) has received and stored information from the DNS-AS server.

Procedure

Use the show ip nbar classification auto-learn dns-as-client 100 detailed command to display the application information that a router has received from the DNS-AS server, arranged by domain.

See Diagnostic Tool: Display Information Learned from the DNS-AS Server.

Results

Expected result: The table has entries that match the information provided by the DNS-AS server.

Step 7: Verify the trusted domains

Check the configured trusted domains on the router. The router sends a DNS request to the DNS-AS server only for applications specified as trusted domains.

Procedure

See Diagnostic Tool: Check Trusted Domains Configured on Router.

Results

Expected result: The show run | sec trusted-domains output shows the configured regular expressions that are used by DNS packet snooping to identify the applications being configured with the DNS-AS feature.

Step 8: Check the binding table

The DNS-AS binding table is regenerated on the router every 5 minutes, by default. This is the “customization interval,” the time during which the router collects auto-learn raw data before creating new custom protocols.

Verify that the auto-custom protocol table reflects the information received from the DNS-AS server.

Procedure

Use the show avc dns-as client binding-table command to display the auto-learn table.

Results

Expected results:

- The table has entries
- The entries match the info displayed in Step 6: Verify that router has received information from the DNS-AS server.

```
Router#show avc dns-as client binding-table
DNS-AS generated protocols:
 Max number of protocols      :50
 Customization interval [min] :5

 Age            :   The amount of time that the entry is active
 TTL            :   Time to live which was learned from DNS-AS server
 Time To Expire :   Entry expiration time in case router does not see DNS traffic for the entry host

 ------------------------------------------------------------------------------------------------------------
 |          |    |            |                      |     |                                                |     | Time to |
 | Protocol| Vrf| Ip List    | Host                 |Age  |  Text record                                   | TTL | Expire  |
 |  name    |    |            |                      |[min]|                                                |[min]| [min]   |
 ------------------------------------------------------------------------------------------------------------
 | hose     |Mgt |2.1.40.207  |hose.nbar-dns-as.com  |1147 |app-name:hose|app-class:MULTIMEDIA-STREAMING |1440 |1437     |
 | hshp     |Mgt |2.1.50.76   |hshp.nbar-dns-as.com  |1147 |app-name:hshp|app-class:BROADCAST-VIDEO      |1440 |1436     |
 | hsjo     |Mgt |2.1.50.127  |annk.nbar-dns-as.com  |1147 |app-name:hsjo|app-class:MULTIMEDIA-STREAMING |1440 |1435     |
 | aplx     |Mgt |20.0.38.235 |hyjn.nbar-dns-as.com  |1147 |app-name:aplx |app-class:NETWORK-CONTROL     |1440 |1436     |
 | annk     |Mgt |20.0.33.14  |cgfo.nbar-dns-as.com  |1147 |app-name:annk|app-class:NETWORK-CONTROL      |1440 |1437     |
```

Step 9: Verify custom protocols

Verify that DNS-AS is generating custom protocols for the applications configured to operate with DNS-AS. Also verify that the traffic for those applications is directed to the IP addresses specified by the DNS-AS server.

Procedure

Use the show ip nbar protocol-discovery stats packet-count command to display the packet count for all NBAR protocols, including the custom protocols generated by DNS-AS.

Results

Expected result: Output displays the custom protocols and shows an increasing packet count.

```
Router#show ip nbar protocol-discovery stats packet-count
 GigabitEthernet0/0/1

 Last clearing of "show ip nbar protocol-discovery" counters 19:00:05

                                     Input                  Output
                                     -----                  ------
   Protocol           Packet Count             Packet Count
   ------------------------ ------------------------ ------------------------
    hose                        100                                      0
    hshp                        200                                      0
    hsjo                        200                                      0
    aplx                        200                                      0
    annk                        200                                      0
```

Step 10: On the DNS-AS server, verify the TXT records

On the DNS-AS server, verify that the TXT records have been configured correctly, according to the rules for specifying NBAR DNS-AS records. If the TXT record is not configured correctly, the router will not learn the classification information specified in the TXT records.

Procedure

The procedure will vary, according to the OS and DNS software operating on the DNS-AS server. In general terms, inspect the TXT records specified on the server.

- The CISCO-CLS is case-sensitive. Verify that it is capitalized.
- Verify the syntax.

Example: For a DNS server using BIND as the DNS server software, a valid entry for an application called staffonly might appear as follows:

```
staffonly    IN A    2.2.2.11
staffonly    IN TXT "CISCO-CLS=app-name:staffonly|app-class:BULK-DATA"
```

Legal Information