# DNS-AS

**Important** Beginning with Cisco IOS XE Fuji 16.9.1, this feature has been deprecated. The functionality has moved to Cisco Software-Defined AVC (SD-AVC).

DNS-AS, "DNS as Authoritative Source," provides centralized control of custom application classification information.

This module contains concepts and tasks for configuring and using DNS-AS.



# Introduction

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.

### Classification Metadata Reflects Organizational Needs, Policy Intent

Different enterprises have different requirements for reporting and shaping traffic through network traffic policy. This is partly because they use different local applications internal to the organization, and partly because widely used applications may have a different business relevance to different organizations.

Consequently, it is often helpful to customize application classification information to determine how network traffic is reported and shaped by traffic policy.

### Leveraging DNS Infrastructure

DNS-AS leverages the universally available DNS query/response infrastructure to enable local DNS servers within an organization to propagate application classification information to routers in an enterprise network. The local DNS servers function as "authoritative source" for both DNS data and custom classification data.

Through its flexibility and simplicity, DNS-AS unlocks traffic reporting and shaping functionality that may otherwise be difficult to configure.

# DNS-AS In Use

### Setup

DNS-AS setup includes configuration steps on the local DNS server(s) and routers within the enterprise network.

Local DNS servers are configured with the classification information for specific "trusted domain" sites/applications. This enables a network administrator to control how a network handles traffic for these local, server-based applications - for example, those used in an enterprise intranet.

Routers are configured to detect DNS traffic for the "trusted domains" (sites/applications) controlled by DNS-AS.

### Propagating Classification Information

When configuration is complete, the DNS servers can provide classification information for the "trusted domain" applications.

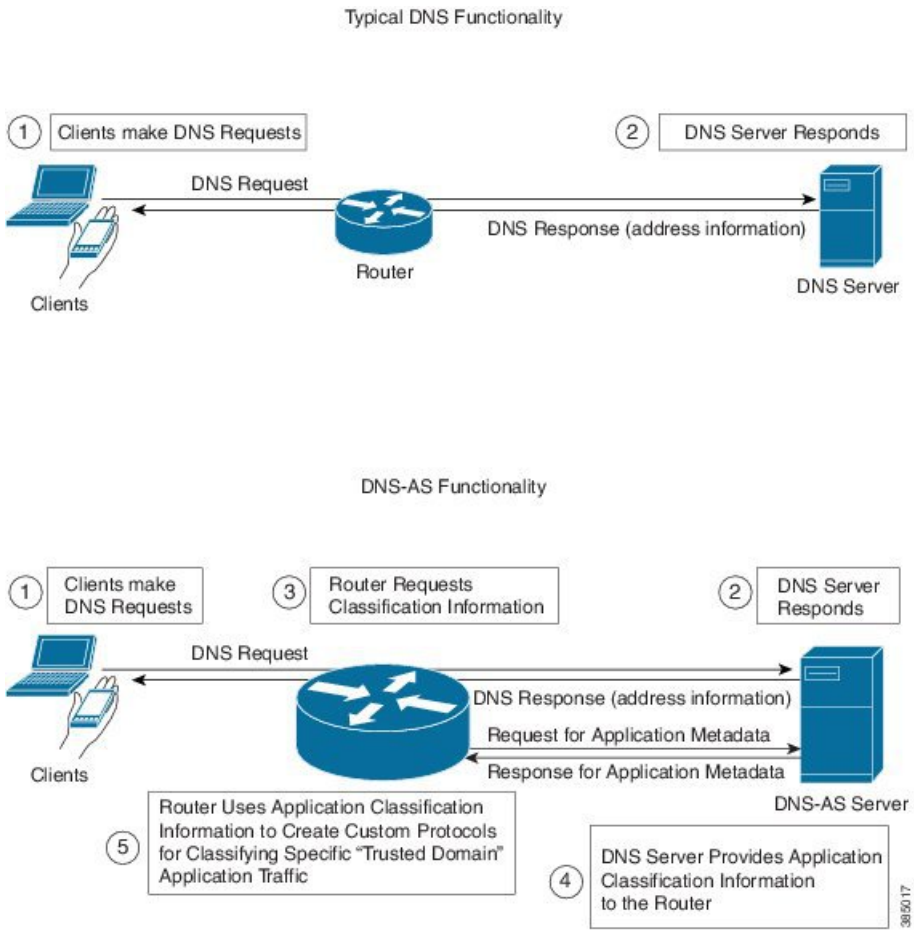
When a client in the network makes a DNS request, the DNS response is sent as usual. If the request relates to a "trusted domain" application, the router then queries the local DNS server about the application. The DNS server sends the router the network address data and the relevant classification information.

### Using the Classification Information

On the routers that receive the information, NBAR2 uses the information to automatically create custom protocols that classify the traffic.

Traffic classification affects application visibility functions, such as reporting of traffic, and it affects application control, such as the use of QoS traffic-shaping policy.

*Figure 1: DNS-AS Functionality*




### Priority

Custom application protocols have priority over standard Cisco NBAR2 Protocol Pack protocols, so it is possible to override Protocol Pack protocols by configuring application classification metadata using DNS-AS.

# Predefined Protocols and Customized Protocols

For most network traffic, the predefined protocols in the NBAR2 Protocol Pack are sufficient to identify and classify traffic.

For local applications not covered by the Protocol Pack, such as the sites and applications in an enterprise's intranet, DNS-AS provides a centralized mechanism for controlling traffic.

# Classification and Traffic Policy

Application classification and traffic policy are related but distinct. DNS-AS provides classification information, but does not directly control traffic policy.

Classification of applications may be controlled by:

- Cisco-provided Protocol Pack
- User-defined protocols
- Automatically-generated custom protocols
- DNS-AS-specified application metadata that indirectly creates custom protocols

Traffic policy may be defined by:

- Direct configuration of policy on the router
- Network controller, such as SDN, providing traffic policy

The following table clarifies the different types of protocols that can control classification of applications.

***Table 1: Protocol Types that Control Application Classification***

| Protocol Type | Source |
|---|---|
| NBAR2 Protocol Pack protocols | Cisco-provided |
| Custom protocols defined manually | User-defined on router |
| Custom protocols defined automatically using DNS-AS | User-defined<br>• Application metadata configured on DNS-AS server(s)<br>• Trusted domains configured on router(s) |

# Efficient, Centralized Configuration

An advantage to using DNS-AS is efficiency of configuration. DNS-AS helps to control application classification over the entire enterprise network, but most of its configuration tasks are handled on the local DNS-AS server(s) operating within the network.

Configuration tasks include:

- **Configuring application metadata**: Defining the metadata for each “trusted domain” application during DNS-AS server setup; modifying the metadata at any time.
- **Configuring trusted domains**: Trusted domains are configured on the individual routers within the network.

### Adaptability

Centralized configuration makes it easier to adapt to changes in the local applications. For example, if the IP addresses of the servers handling a local application change, or if the metadata attributes (application-class, business-relevance, and so on) for an application change, you can configure the changes on the local DNS-AS server(s) and the updates are propagated to the routers throughout the entire network.

# DNS-AS vs. SDN Controller Functionality

DNS-AS and SDN controllers, when used, both operate broadly on the network. While an SDN controller provides traffic policy to devices in the network, DNS-AS provides application-match metadata.

# NBAR2 Responding to Evolving Networks and Network Traffic

### Applications Using End-to-End Encryption

Many of today's network applications operate in clear text over common transports such as HTTP. These applications can be identified using Deep Packet Inspection (DPI), a resource-intensive method. However, more and more network applications are communicating with end-to-end encryption, preventing identification by DPI.

### Enterprise Networking Moving to the Cloud

A trend in enterprise networks is moving to the cloud. Instead of operating their own full-scale enterprise network, organizations are opting to move network infrastructure to cloud service providers. Their downsized internal network may have to control a variety of network devices located anywhere in the world. Those devices, managed by the cloud services provider, may not be under their direct administrative control.

### NBAR Flexibility, Agility

Cisco NBAR2 features, such as DNS-AS, are evolving to address the changing trends in enterprise networking. While end-to-end encryption and migration to the cloud complicate the task of providing application visibility and control, NBAR continues to aim for:

- Simplicity in network configuration
- Agility at scale

# Comparison with the Custom Protocol Feature

The DNS-AS configuration process is similar in some ways to using the NBAR2 **custom protocol** feature to create a protocol for a specific application relevant to the organization, but DNS-AS does not operate router-by-router for each individual application.

DNS-AS also provides an easier method of reconfiguring how numerous devices within the network handle custom applications.

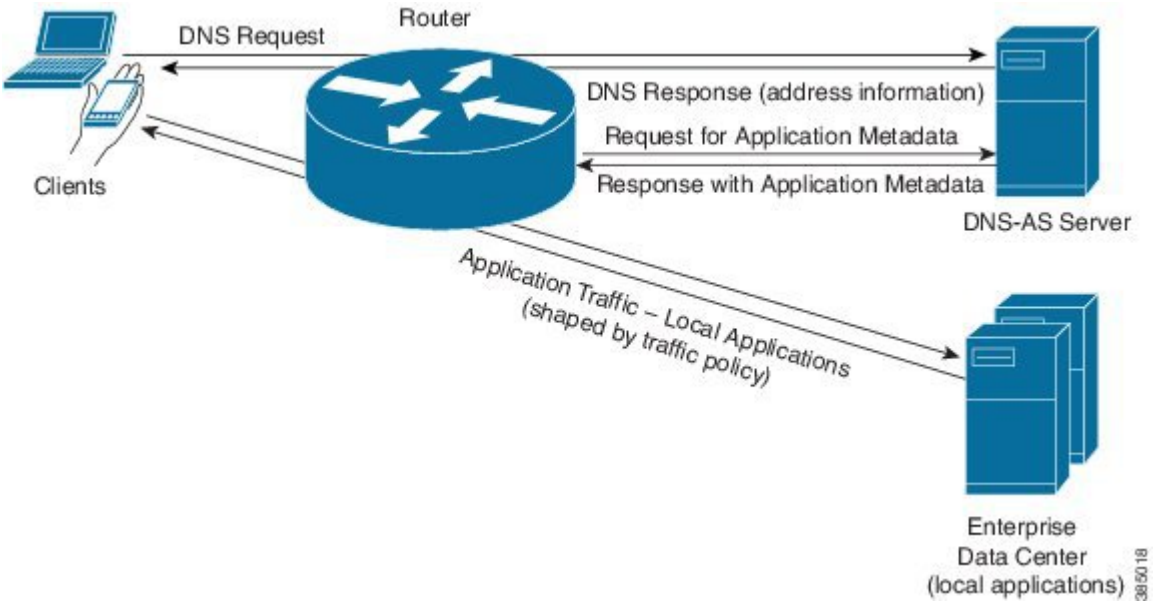
- When using the **custom protocol** feature, if any attributes of a custom application change, or if the server hosting the application changes, then updates to the custom application protocol must be made on each router in the network, one by one. In a network containing hundreds of routers, this process is impractical.
- When using **DNS-AS**, the single reconfiguration on the DNS server propagates information to all routers in the network.

# DNS-AS Mechanism

## Basic Topology

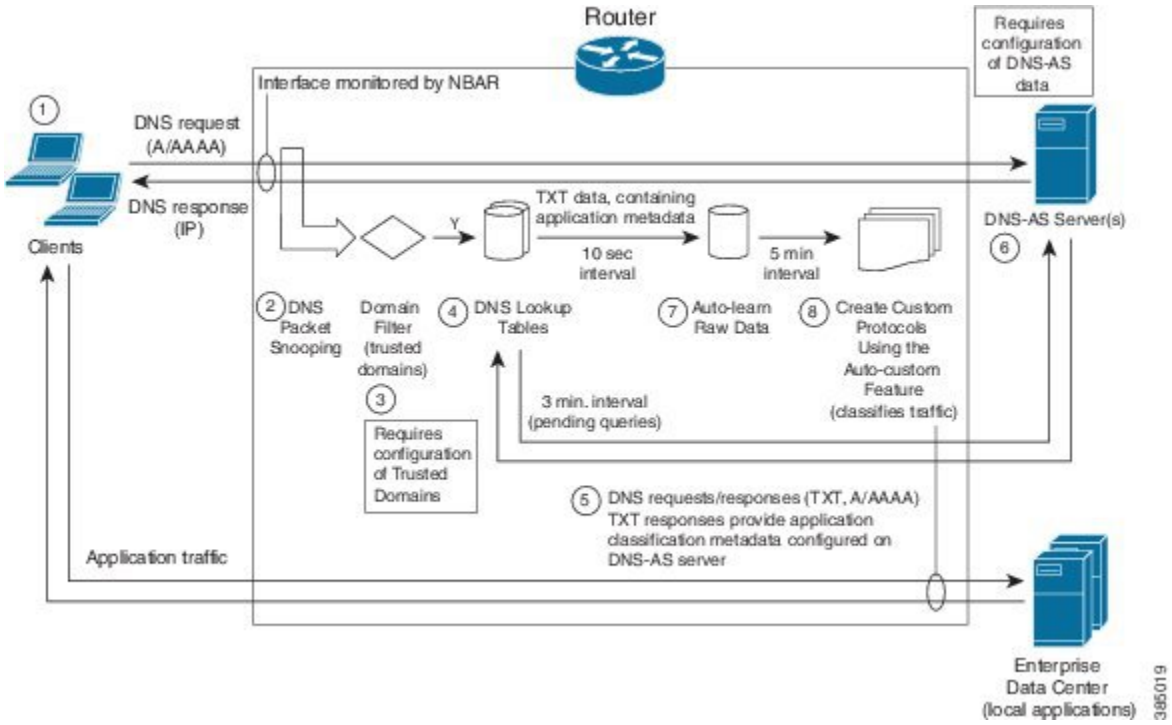
The following figure illustrates how the DNS-AS server operates with the clients (user devices), routers, and data centers (hosting local applications) within an enterprise network.

***Figure 2: Topology***



## Mechanism Details

*Figure 3: Details of Mechanism*




**1**. A client (PC in the network) makes a request for a domain defined as a trusted domain. The request goes to the router to which the client is connected.

**Example**: A browser requests: StaffOnly.XYZ.com

**2**. Operating on the router, NBAR2 uses DNS packet snooping (on interfaces on which NBAR2 is active) to monitor the DNS requests from clients in the network. The router forwards the information in the DNS requests to the next step, which analyzes the data.

**3**. The Domain Filter mechanism identifies DNS requests for a trusted domain by matching to configured textual regular expressions.

**Example regular expression**: *staffonly.xyz.com

**4**. For each trusted domain identified in the previous step, the router prepares a "TXT" DNS request to send to the DNS-AS server. It collects these "pending" requests for a brief performance-optimizing interval.

**5**. The router server sends the "TXT" DNS requests to the DNS-AS server.

**6**. The DNS-AS server sends the "TXT" response. If the "TXT" response contains information with the "CISCO-CLS" prefix, the router sends an A request (requesting an IPv4 address) or an AAAA request (requesting an IPv6 address). The DNS-AS server sends an A or AAAA response to the request.

**7**. The router collects the "auto-learn raw data" responses containing application classification data for a brief interval.

**8**. Using the auto-learn raw data, NBAR creates custom application protocols for the relevant domains. Note: Custom application protocols have priority over standard Cisco NBAR2 Protocol Pack protocols.

### DNS-AS Server Always Provides the Latest Version

If the router later makes a new request for a previously queried domain, the DNS-AS server sends the latest version of the metadata. So if the metadata has changed, the router will receive the new version.

# DNS-AS Setup

DNS-AS requires configuration on local DNS servers and routers, as follows.


- DNS-AS Server Setup, on page 8
- DNS-AS Router Setup, on page 9


# DNS-AS Server Setup

On local DNS servers within the enterprise network, configure application classification information for each "trusted domain." This is the information that the server propagates to routers when queried for application metadata. When the router sends a TXT query regarding an application, the DNS server sends the relevant metadata in the TXT response.

### Application Metadata Fields

Application metadata is configured on the DNS-AS server(s). The individual routers in the network apply the metadata to create custom protocols and handle application traffic accordingly.

The following table describes the metadata fields that can be specified for applications handled by the DNS-AS feature. Customized application metadata specified using the DNS-AS feature has priority over any metadata provided by the NBAR2 Protocol Pack installed on a router.

***Table 2: Metadata Fields***

| Field | Mandatory/Optional | Usage Notes |
|---|---|---|
| Application name<br>(app-name) | Mandatory | For an application **included** in the installed Protocol Pack: Any customized metadata specified for the application takes priority over metadata specified in the Protocol Pack.<br>For an application **not included** in the installed Protocol Pack: A new custom-protocol is created. |
| Application ID<br>(app-id) | Mandatory | If not specified, NBAR2 generates an application-id.<br>Not valid for existing applications.<br>**Note** It is recommended to include this field when specifying a new application. This provides a universal ID number for the customized application within the network. The universal ID number enables traffic data collectors to aggregate DNS-AS custom application classification data coming from different devices within the network. |

| Field | Mandatory/Optional | Usage Notes |
|---|---|---|
| Traffic class<br>(app-class) | Optional | If this field is specified and the business-relevance field is not specified, NBAR2 automatically assigns the business-relevance field a value of "business-relevant".<br>**Note** It is strongly recommended to include this field when specifying a new application. Without specifying traffic-class, the application uses the default traffic-class value. |
| Business relevance<br>(business) | Optional | Business relevance |

# DNS-AS Router Setup

On Cisco routers operating in the network, activate the DNS-AS feature and configure the DNS-AS server(s) to use, as well as the "trusted domains," as follows:

### Step 1: Activate DNS-AS on Routers in the Network

On the routers in the network, activate DNS-AS.

```
avc dns-as client enable
```

### Step 2: Specify the DNS-AS Server(s) to Use

Specify the DNS-AS server(s) to query with TXT requests for classification metadata.

```
ip name-server vrf <name> <address>
```

For details, see Configuring the DNS-AS Server for a Router to Query, on page 11.

### Step 3: Configure Trusted Domains on Routers in the Network

On the routers in the network, configure "trusted domains." The DNS-AS feature affects only the applications configured as trusted domains.

When a router detects DNS traffic for a trusted domain, it requests and receives application classification metadata from the local DNS-AS server using TXT request/response.

Configure trusted domains by providing textual regular expressions that will match domain names found in DNS requests sent by clients in the network. For the example above, **StaffOnly.XYZ.com**, the regular expression might be:

```
*staffonly.xyz
```

For details, see Configuring Trusted Domains, on page 12.

# Deploying a New Application in the Network

When deploying a new local application in the organization's network, review the procedures for setting up DNS-AS to add the new application to the DNS-AS server setup and the router "trusted domain" setup.

# Restrictions

The following restrictions apply to using DNS-AS:

- Only IPv4 DNS servers are supported.
- Maximum of 50 DNS-AS custom-applications are supported (across all DNS servers within the network).

**Note** NBAR2 supports a total of 120 custom protocols. Custom protocols generated by DNS-AS count toward the total.

- Maximum of 2 VRFs are supported.
- Maximum of 2 servers are supported per VRF.
- NBAR performs DNS packet snooping only on DNS traffic on interfaces on which NBAR is configured.
- A DNS-AS custom-application protocol can include either IPv4 addresses or IPv6 addresses, but not both.
- When using DNS-AS to customize existing applications, the "app-id" field should either be omitted from TXT record or be identical to the exiting application "app-id".
- For applications that are not included in the NBAR2 Protocol Pack, the "app-name" field must be unique across all TXT records across all DNS-AS servers.

# DNS-AS CLI Commands

Several CLIs are used on routers in the network to configure and monitor DNS-AS.

See the following sections:

- Activating and Configuring DNS-AS, on page 10
- Monitoring DNS-AS, on page 15

## Activating and Configuring DNS-AS

The following reference table provides a summary of DNS-AS configuration commands.

*Table 3: Configuration Commands*

| CLI | Description |
|---|---|
| **ip name-server vrf** *name address* | Configures the DNS server.<br>When used for other router functions, this CLI can support several VRFs, and up to 6 IP addresses per VRF. However, DNS-AS supports only 2 VRFs, and the first 2 servers configured per VRF.<br>**Usage Notes**:<br>• The specified VRF does not have to be defined at the time that the CLI is executed.<br>• Configuration of more than one server is used for redundancy or VRF.<br>• Immediately after configuration, DNS-AS prioritizes the configured servers in the order in which they were configured. After restarting the router, DNS-AS prioritizes in alphabetical order, using the VRF name.<br>• You can view the configuration using the **show avc dns-as client name-server brief** command. This indicates which servers the DNS-AS feature is using. |
| 1. **avc dns-as client trusted-domains**<br>2. **domain** *regular-expression* | Configures trusted domains, using a regular expression as a filter.<br>**Usage Notes**:<br>Can configure up to 50 trusted domains.<br>**Example**:<br>`Device(config)#avc dns-as client trusted-domains`<br>`Device(config-trusted-domains)#domain *staffonly.xyz.com`<br>`Device(config-trusted-domains)#exit` |
| **avc dns-as client enable** | Enables DNS-AS. |
| 1. **interface** *interface*<br>2. **avc dns-as learning** | Enables NBAR on an interface.<br>The DNS-AS feature is only active on interfaces monitored by NBAR. If NBAR has been activated on an interface for use with any NBAR feature, the interface will be monitored for DNS-AS also.<br>**Example**:<br>`Device#config terminal`<br>`Device(config)#interface gig 0/0/0`<br>`Device(config-if)#avc dns-as learning`<br>`Device(config-if)#exit` |

## Configuring the DNS-AS Server for a Router to Query

Use the following procedure on a router to configure the DNS-AS server(s). For information about displaying the configured DNS servers, see Displaying Active DNS Servers, on page 19.

**SUMMARY STEPS**

1. **configure terminal**
2. **ip name-server vrf** *name address*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 2** | **ip name-server vrf** *name address*<br>**Example:**<br>This example specifies a DNS server called MANAGEMENT.<br>`Device(config)#ip name-server vrf MANAGEMENT 10.56.56.56` | Specifies the DNS server. |

## Configuring Trusted Domains

The DNS-AS feature operates only on applications configured in the trusted domain list.

Configure trusted domains by specifying regular expressions to match the domain name—for example, ***cisco.com** for all Cisco.com traffic, including **www.cisco.com** and **developer.cisco.com**.

When specifying trusted domains, it may be helpful to use a packet analyzer application, such as the open-source Wireshark application, to examine DNS request packets for trusted applications. The domain name appears in the packet and can be used for building effective regular expressions.

Use the following procedure on a router to configure a new trusted domain.

**SUMMARY STEPS**

1. **configure terminal**
2. **avc dns-as client trusted-domains**
3. **domain** *regular-expression*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 2** | **avc dns-as client trusted-domains**<br>**Example:** | Enters trusted domain configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)#avc dns-as client trusted-domains` | |
| **Step 3** | **domain** *regular-expression*<br>**Example:**<br>`Device(config-trusted-domains)#domain *staffonly.xyz.com` | The regular expression specifies the domain. |

## Enabling DNS-AS

Use the following procedure on a router to enable the DNS-AS feature.

### SUMMARY STEPS

1. **configure terminal**
2. **avc dns-as client enable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 2** | **avc dns-as client enable**<br>**Example:**<br>`Device(config)#avc dns-as client enable` | Enables the DNS-AS feature. |

## Disabling DNS-AS

Use the following procedure on a router to disable the DNS-AS feature.

### SUMMARY STEPS

1. **configure terminal**
2. **no avc dns-as client enable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **no avc dns-as client enable**<br>**Example:**<br>`Device(config)#no avc dns-as client enable` | Disables the DNS-AS feature. |

## Enabling NBAR on an Interface for DNS-AS

When using DNS-AS, each router in the network must snoop DNS traffic from clients in the network and forward the data to the next step of the DNS-AS process, the domain filter.

For the router to monitor the DNS requests, NBAR must be enabled on the interfaces on which the router receives DNS requests from clients. As a general rule, the router monitors DNS traffic on all interfaces on which NBAR is enabled.

Numerous CLIs can enable NBAR on an interface. When using DNS-AS, use the following procedure to enable NBAR on the interface for DNS-AS learning.

**Note** In cases where NBAR is already enabled on the interface, this task is redundant. For example, if IP protocol discovery is already enabled on the interface, the procedure is not necessary. However, for clarity, even in these redundant situations, it is recommended to use this procedure.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface*
3. **avc dns-as learning**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface** *interface*<br>**Example:**<br>`Device(config)#interface gig 0/0/0` | Enter interface configuration mode for a specific interface. |
| **Step 3** | **avc dns-as learning**<br>**Example:**<br>`Device(config-if)#avc dns-as learning` | Enable NBAR on the interface specified in a previous step. |

# Monitoring DNS-AS

The following reference table provides a summary of DNS-AS monitoring commands.

***Table 4: Monitoring Commands***

| CLI | Description |
|---|---|
| **show avc dns-as client statistics** | Show receive/transmit counters per server. |
| **show avc dns-as client binding-table** | Show DNS-AS custom-application data. |
| **show avc dns-as client binding-table detailed** | Show DNS-AS custom-application data in a record format. |
| **clear avc dns-as client statistics** | Clear the receive/transmit counters. |
| **show avc dns-as client name-server brief** | Show configured DNS servers. |
| **show ip nbar classification auto-learn dns-as** *<1-100>* | Show the auto-learn table.<br>The number specifies the number of entries to display in the table. |
| **clear ip nbar classification auto-learn dns-as-client statistics** | Clear the auto-learn table. |
| **clear ip nbar classification auto-learn dns-as restart** | Restart all DNS-AS learning. All databases are cleared. |
| **show ip nbar classification auto-learn dns-as pending-queries** | Show pending queries. |
| **clear ip nbar classification auto-learn dns-as pending-queries** | Clear pending-queries statistics.<br>**Usage Notes**:<br>This CLI does not cause injection of pending queries. |
| **show ip nbar protocol-discovery stats packet-count** | Display the packet count for all NBAR protocols, including the custom protocols generated by DNS-AS. |

## Showing DNS-AS Client Statistics

Use this procedure to display DNS-AS client statistics. The results display the running total of number of packets, and are displayed per server.

**Usage**:

- Disabling DNS-AS resets the statistics.
- In some cases, unusually high traffic volume may cause some statistics to fail, in which case the command output displays "Error" for some statistics.

### SUMMARY STEPS

1. **show avc dns-as client statistics**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show avc dns-as client statistics**<br>**Example:**<br>`Device#show avc dns-as client statistics`<br>`csi-mcp-asr1k-02#show avc dns-as client statistics`<br>`Server details: vrf-id = 2 vrf-name = MNG ip = 10.56.196.50`<br>`AAAA Query Error packets 0`<br>`AAAA Query TX packets 0`<br>`AAAA Response RX packets 0`<br>`TXT Query Error packets 0`<br>`TXT Query TX packets 50`<br>`TXT Response RX packets 50`<br>`A Query Error packets 0`<br>`A Query TX packets 50`<br>`A Response RX packets 50`<br>`Total Drop packets 0`<br>`Server details: vrf-id = 5 vrf-name = vrf2 ip = 10.56.196.51`<br>`AAAA Query Error packets 0`<br>`AAAA Query TX packets 0`<br>`AAAA Response RX packets 0`<br>`TXT Query Error packets 0`<br>`TXT Query TX packets 0`<br>`TXT Response RX packets 0`<br>`A Query Error packets 0`<br>`A Query TX packets 0`<br>`A Response RX packets 0`<br>`Total Drop packets 0` | Display client statistics, per server. |

## Showing the DNS-AS custom-application Data

Use this procedure to display DNS-AS custom-application data in **binding table format**. Also see the **detailed** form of the command, which presents the same information in **record format**, which enables piping the data into another application. See Showing the DNS-AS custom-application Data – Detailed, on page 17.

The information includes:

- Maximum number of protocols that can be customized using DNS-AS.
- Customization interval—Interval during which the router collects auto-learn raw data before creating new custom protocols. Default: 5 minutes
- Table of protocols currently stored in the binding table, with the VRF name, server IP, age, metadata, TTL, and Time to Expire data.

#### When Do Protocols Reach This Table?

The DNS-AS process has built-in rate limiters that introduce short delays to optimize overall performance. The major intervals that affect when protocols appear in the binding table are (total of about 8 minutes by default):

- Rate limiter before router sends DNS request to the DNS server (default: 3 minutes).
- Rate limiter after the router receives a DNS response from the DNS server (default: 10 seconds).
- Rate limiter before collected raw data is used to generate custom-protocols (default: 5 minutes).

### SUMMARY STEPS

1. **show avc dns-as client binding-table**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show avc dns-as client binding-table**<br>**Example:**<br>`Device#show avc dns-as client binding-table` | Displays a binding table populated by custom-application data. |

## Showing the DNS-AS custom-application Data – Detailed

Use this procedure to display DNS-AS custom-application data in a record format, which enables piping the output into another application.

This procedure uses a command identical to the one described for the Showing the DNS-AS custom-application Data, on page 16 procedure, but with addition of the **detailed** keyword:

**show avc dns-as client binding-table detailed**

The following example uses the sec command in a UNIX-like environment to select output for the xyz domain. The command output is piped to sec, which filters for **staffonly**.

```
Device#show avc dns-as client binding-table detailed | sec staffonly
Protocol-name        : staffonly
 VRF                 : MNG
 Host                : staffonly.xyz.com
 Age[min]            : 17
 TTL[min]            : 1440
 Time to Expire[min] : 1420
 TXT Record          : app-name:staffonly|app-class:BULK-DATA
 IP                  : 10.2.3.10
```

## Clearing the Receive and Transmit Counters

Use this procedure to clear the receive and transmit counters for the DNS-AS client statistics.

### SUMMARY STEPS

1. **clear avc dns-as client statistics**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **clear avc dns-as client statistics**<br>**Example:**<br>`Device#clear avc dns-as client statistics` | Clears receive and transmit counters. |

## Clearing the auto-learn Table

Use this procedure to clear the auto-learn raw data.

The auto-learn raw data is collected in the control plane for an interval (default 5 minutes) before being sent to the mechanism that creates custom protocols based on the data. Shortly after being cleared (typically within 10 seconds), the table is regenerated when the same data or a subset of the data, is sent again from the data plane, where the data typically has a 24-hour TTL, back to the auto-learn raw data table in the control plane.

By contrast, using the Clearing and Restarting DNS-AS Learning, on page 18 procedure clears the auto-learn raw data and any custom-protocols that have been created.

**SUMMARY STEPS**

1. **clear ip nbar classification auto-learn dns-as-client statistics**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **clear ip nbar classification auto-learn dns-as-client statistics**<br>**Example:**<br>`Device#clear ip nbar classification auto-learn dns-as-client statistics` | Clears the auto-learn raw data. |

## Clearing and Restarting DNS-AS Learning

Use this command to clear the auto-learn raw data and any custom protocols that have been generated. All databases are cleared and the auto-learn process restarts without any prior data.

**SUMMARY STEPS**

1. **clear ip nbar classification auto-learn dns-as restart**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **clear ip nbar classification auto-learn dns-as restart**<br>**Example:**<br>`Device#clear ip nbar classification auto-learn dns-as restart` | Clears the auto-learn raw data and any custom protocols that have been generated. |

## Displaying Active DNS Servers

Use this procedure to display the DNS servers configured to operate with DNS-AS. For information about configuring DNS servers, see Configuring the DNS-AS Server for a Router to Query, on page 11.

### SUMMARY STEPS

1. **show avc dns-as client name-server brief**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show avc dns-as client name-server brief**<br>**Example:**<br>`Device#show avc dns-as client name-server brief` | Displays the DNS servers configured to operate with DNS-AS. |

## Showing DNS-AS Auto-learn Data

Use this procedure to display the data collected in the DNS-AS auto-learn raw data repository before it has been used to create custom protocols.

For information about clearing the auto-learn data, see Clearing the auto-learn Table, on page 18.

**When Does Data Reach This Table?**

The DNS-AS process has built-in rate limiters that introduce short delays to optimize overall performance. The major intervals that affect when data reaches the auto-learn step are (total of about 3 minutes by default):

- Rate limiter before router sends DNS request to the DNS server (default: 3 minutes).
- Rate limiter after the router receives a DNS response from the DNS server (default: 10 seconds).

### SUMMARY STEPS

1. **show ip nbar classification auto-learn dns-as-client** <*1-100*> **detailed**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show ip nbar classification auto-learn dns-as-client** <*1-100*> **detailed**<br>**Example:**<br>`Device#show ip nbar classification auto-learn dns-as-client 100 detailed` | Displays the data collected in the DNS-AS auto-learn raw data repository. The number determines how many entries to display in the table. |

## Displaying Pending DNS Queries

Use this procedure to display the DNS queries that the router has not yet sent to the DNS server. A rate limiter limits transmission of accumulated DNS queries to the DNS-AS server to an interval of 3 minutes. This optimizes system performance by not overloading the DNS-AS server with many identical requests.

See the Clearing the Pending DNS Query Statistics, on page 20 procedure for clearing the pending queries statistics.

### SUMMARY STEPS

1. **show ip nbar classification auto-learn dns-as pending-queries**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show ip nbar classification auto-learn dns-as pending-queries**<br>**Example:**<br>`Device#show ip nbar classification auto-learn dns-as pending-queries`<br>`AAAA queries pending inject 0`<br>`AAAA queries injected 0`<br>`TXT queries pending inject 0`<br>`TXT queries injected 50`<br>`A queries pending inject 0`<br>`A queries injected 50` | Display the pending queries. |

## Clearing the Pending DNS Query Statistics

Use this procedure to clear the pending queries statistics. See the Displaying Pending DNS Queries, on page 20 procedure for displaying the statistics.

### SUMMARY STEPS

1. **clear ip nbar classification auto-learn dns-as pending-queries**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **clear ip nbar classification auto-learn dns-as pending-queries**<br>**Example:**<br>`Device#clear ip nbar classification auto-learn dns-as pending-queries` | Clear the pending query statistics. |

# DNS-AS Troubleshooting

For DNS-AS Troubleshooting, see Cisco DNS-AS Troubleshooting.