



DNS

Teldat-Dm 723-I

Copyright© Version 11.06 Teldat SA

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I	Related Documents.	1
Chapter 1	Domain Name System	2
1.1	Introduction	2
1.2	Domain resolution	2
1.2.1	Domain name resolver operation	3
1.2.2	Domain name server operation	4
1.2.3	Teldat router operations	4
1.2.4	DNS resource records.	5
1.2.5	DNS Messages.	6
1.3	References	9
Chapter 2	Configuring DNS	10
2.1	Configuring DNS	10
2.1.1	CACHE	10
2.1.2	LIST	11
2.1.3	N-RETRANSMISSIONS	14
2.1.4	NO	14
2.1.5	PERMANENT-ENTRY.	16
2.1.6	PROBE	17
2.1.7	RESOLVER-PORT	18
2.1.8	SERVER	18
2.1.9	SERVER-PORT	18
2.1.10	SERVERS-CHECKING	19
2.1.11	SOURCE-ADDRESS	19
2.1.12	T-RETRANSMISSIONS	19
2.1.13	EXIT	19
Chapter 3	Monitoring DNS.	20
3.1	Monitoring DNS	20
3.1.1	LIST	20
3.1.2	LOOKUP	21
3.1.3	CACHE	22
3.1.4	PROBE	28
3.1.5	EXIT	28

I Related Documents

Teldat-Dm710-I PPP Interface

Teldat-Dm775-I VRF-Lite Feature

Chapter 1 Domain Name System

1.1 Introduction

The Domain Name System, more commonly referred to as DNS, is a standard protocol described in RFCs 1034 and 1035. It allows network users to use simple hierarchical names to refer to other devices. This way, the user can avoid the device's IP address and refer to it using a name that is easier to remember. It also makes changing a device's IP address easier: changes of address should only be passed along to the DNS server managing said device, with this taking place transparently to the user, who will keep on using the same name to refer to the device.

DNS is an application protocol and uses both UDP and TCP. To speed up communication, clients use UDP to query DNS servers and only use TCP if they receive a truncated DNS response.

DNS uses the concept of a *distributed name space*. Symbolic names are grouped into *zones of authority*, more commonly known as *zones*. In each of these zones, one or more hosts are tasked with maintaining a database of symbolic names and IP addresses and providing a server function for clients who wish to convert symbolic names to IP addresses. These local *name servers* are logically interconnected in a *domain* tree hierarchy. Each zone contains a part, or a *subtree*, of the hierarchical tree and the names within a zone are administered separately from those in other zones. Name servers have authority over zones. Where a domain contains a subtree that falls in a different zone, the authoritative name servers of the top-level domain *delegate authority* to the authoritative name servers of sub-domains. Name servers can also delegate authority to themselves; in this case, the name space is still divided into zones, but authority for two zones is held by the same server.

The results of this scheme are:

- Rather than having a central name server for the database, the task of maintaining it is shared between the hosts throughout the name space.
- The authority for creating and changing symbolic host names, and the responsibility for maintaining a database for them, is placed with the owner of the zone holding the host names.
- From the user's point of view, there is only one database dealing with address resolution.

1.2 Domain resolution

Domain name resolution is a client-server process. The typical DNS client queries name servers to resolve domain names into associated IP addresses. These types of queries are called standard requests. There are also inverse requests to resolve an IP address into a domain name and generic requests to obtain additional data on a domain.

There are two types of resolvers:

- Full resolver: the resolver itself. This makes the necessary queries to obtain the desired information. It analyzes server responses to see if it has received a response to the query made or a delegation to another server. In the latter case, it keeps transmitting queries until it gets the desired response.
- Simple resolver (stub resolver): this delegates the resolution query to a full resolver. The simple resolver has a list of server IP addresses capable of performing the resolution process in full. It sends the DNS query and waits for a response, refusing responses that contain delegations to other servers.

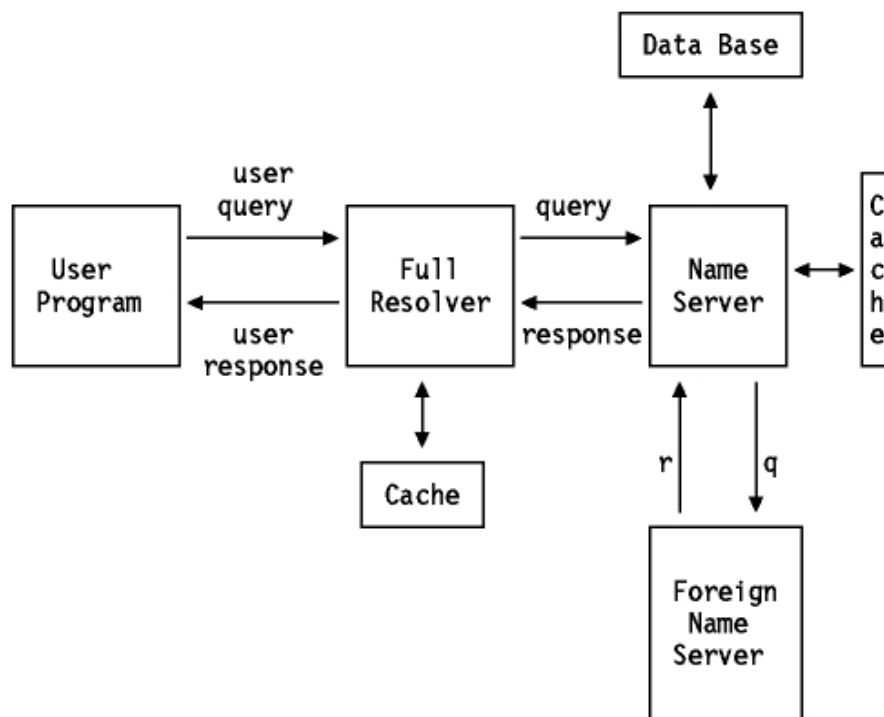


Fig. 1: Operating scheme of the full resolver

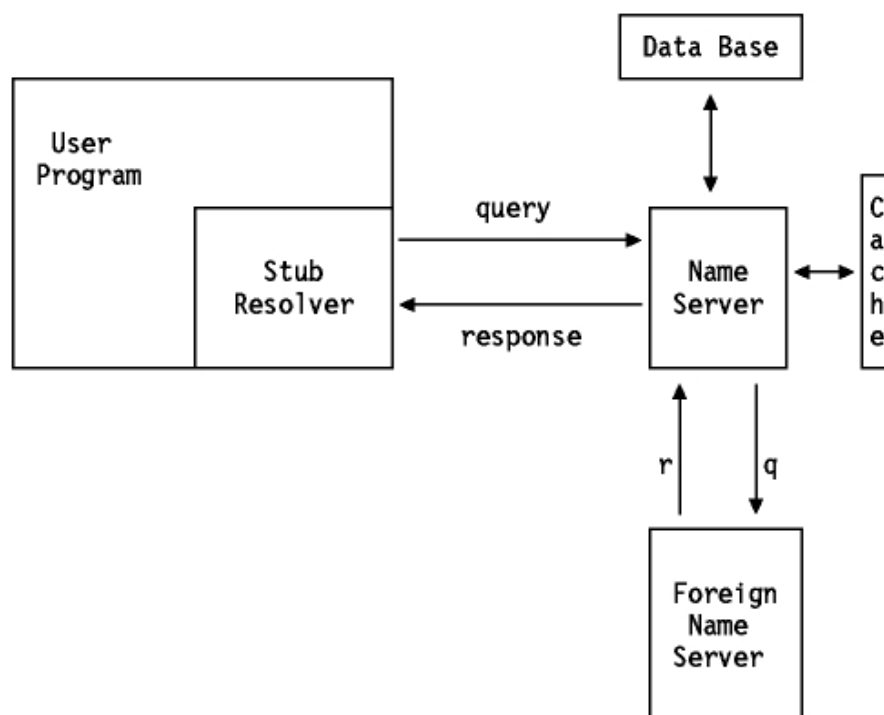


Fig. 2: Operating scheme of the stub resolver

1.2.1 Domain name resolver operation

There are two types of DNS queries: *recursive* and *iterative* (also known as *non-recursive*). A flag bit in the query specifies whether the client wants a recursive query and a flag bit in the response specifies whether the server supports recursive queries. The difference between recursive and iterative queries arises when the server receives a query that it can't answer by itself. A recursive query requires that the server, in turn, becomes a DNS client for the query; sending out a query to another server to find out the sought-after information and then returning the answer to the client. An iterative query is one in which the name server returns the information it has in its cache, in addition to a list of other servers the client can contact to complete the query.

There are two types of domain name responses: *authoritative* and *non-authoritative*. A flag bit in the response indicates the response type. When a name server receives a DNS query for a domain that is under its zone of authority, it returns a response with the flag bit set. If it does not have authority for the zone, the name server's reaction depends on whether or not the recursive flag is set.

If the recursive flag is set and the server supports recursive queries, it will query another name server. This will either be a name server whose zone of authority includes the query domain or one of the root name servers. If the second server cannot give an authoritative answer, the process is repeated.

When a server (or a full resolver) receives a response, it caches it to improve performance of repeat queries. The cache entry is stored according to the *time to live* (TTL) value specified in the 32-bit TTL field of the response. 172,800 seconds (two days) is a typical TTL value.

If the recursive flag is not set or the server doesn't support recursive queries, it returns the information that it has in its cache (along with a list of servers capable of giving authoritative answers).

1.2.2 Domain name server operation

Each name server has *authority* over zero or more zones. There are three types of name server:

- **primary:** a primary name server has authority over a zone and loads all information for the zone from the disk.
- **secondary:** a secondary name server has authority over a zone but retrieves information for the zone from a primary server using what is called a *zone transfer*. To remain synchronized, the secondary name servers query the primary at regular intervals (typically every three hours) and re-run the zone transfer if the primary has been updated. A name server can operate as a primary or a secondary server for multiple domains, or a primary for some domains and a secondary for others. A primary or secondary server is able to perform all the functions of a cache server.
- **cache:** a name server that does not have authority over any zone is called a cache server. The latter obtains its information from primary or secondary servers. It requires at least one name server (NS) record to point it to a server from which it can initially obtain information.

When a domain is registered with the root and a separate zone established, the following rules apply:

- The domain must be registered with the root administrator.
- The domain must have an identified administrator.
- At least two name servers with authority for the zone must be accessible from inside and outside the domain to avoid single points of failure.

Name servers that delegate authority should also apply these rules, since they are responsible for the behavior of the delegated name servers.

1.2.3 Teldat router operations

The Teldat router acts as a DNS resolver and a DNS relay server.

1.2.3.1 DNS Resolver

As a “resolver”, the Teldat router acts like a DNS client, passing queries generated by the device itself (as a result of, for example, pinging or performing a Telnet connection to a *hostname*) to an external DNS server.

DNS servers are added through the SERVER command. We can configure servers of both family addresses: IPv4 and IPv6. These servers can be configured in a different VRF table (VPN *routing and forwarding*) to the main router table, but only if the server is not IPv6. For further information on how to configure VRF tables, please see the following manual: “Teldat-Dm-775-I VRF-Lite Feature.”

One of the parameters that defines an internal query is the VRF that the resolver must use to make the query. The resolver queries, one by one (if it doesn't receive an answer) only those servers configured in said VRF. Servers that can be accessed through the same VRF are queried in the order in which they were added.

If the cache is enabled (through the CACHE ENABLE command), each time a query is resolved, an entry is added to the cache associated with the VRF used to make the query. This ensures that clients don't repeatedly query the DNS server for the same address as the cache is first checked to see if the answer is already there. An entry remains in the cache for the TTL period specified in the the TTL field.

1.2.3.2 DNS Relay Server

As a DNS Relay server, the router passes client DNS queries on to the servers added with the SERVER command. Thus, the router acts as an intermediary between the clients and the servers.

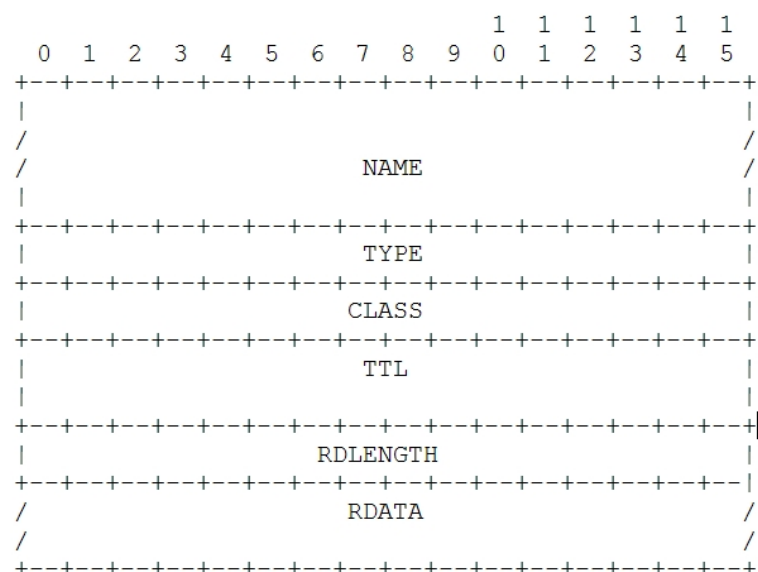
Communication to and from the server can be done using the secondary VRF (VPN *routing and forwarding*) tables

defined in the router, but only if the server is not IPv6. For further information on how to configure VRF tables, please see the following manual: “Teldat-Dm-775-I VRF-Lite Feature.” If no response is received, the servers are queried in the order they were configured in (regardless of the associated VRF).

If the cache is enabled (through the `CACHE ENABLE` command), each time the server resolves a query and sends a response, an entry is added to the default DNS cache (the one associated with the main VRF). This ensures that clients don't repeatedly query the DNS server for the same address, as the cache is first checked to see if the answer is already there. An entry remains in the cache for the TTL period specified in the TTL field.

1.2.4 DNS resource records

The DNS distributed database is made up of *resource records (RRs)*. These match domain names to *network objects*. The most common network objects are host addresses, but DNS is designed to accommodate a diverse range of different objects. The standard resource record format is:



NAME

This is the name of the domain the record refers to. As far as the domain name composition is concerned, DNS rules are very general. A domain name consists of a series of labels made up of alphanumeric characters or hyphens. Each label is between 1 and 63 characters long and starts with an alphabetical character. Domain name labels are usually separated by a period. In messages, labels include a byte at the beginning to indicate the length of the label. All names end with a null (zero-length) label indicating the root domain. Domain names are not case sensitive.

CLASS

Identifies the protocol family. Class 1 (IN) is used for Internet.

TYPE

Identifies the type of record resource. Type 1 (A) specifies a host address. Type 28 (AAAA) specifies an IPv6 Address.

TTL

This stands for *time-to-live* and is the length of time (in seconds) that the name server will store the record in its cache. This is stored in the DNS as an unsigned 32-bit value. 86400 (one day) is a typical TTL value for records pointing to IP addresses.

RDLENGTH

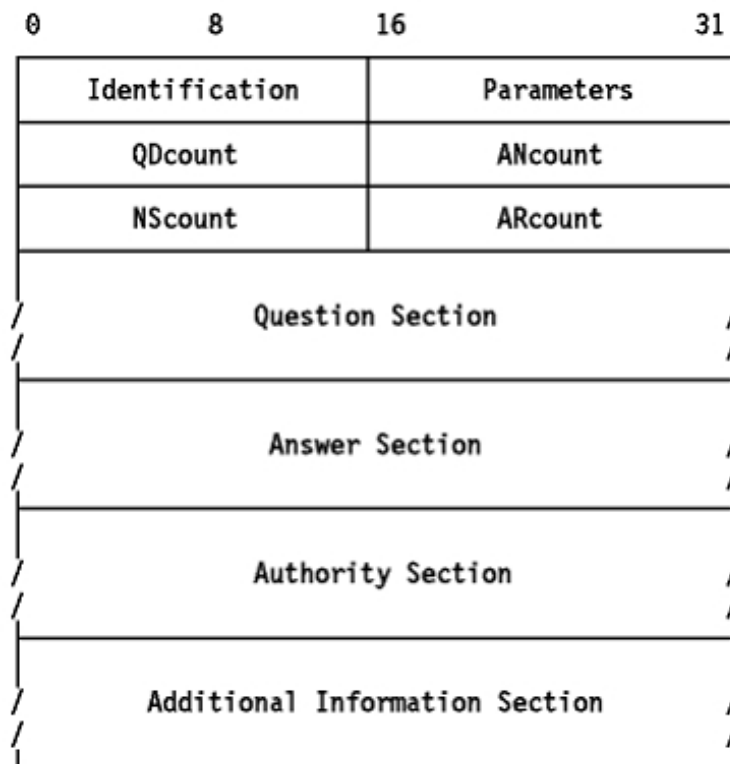
Length of the data part.

RDATA

Record data. The data varies depending on the record type and class. So, for example, for type A and class IN, the data will be four bytes so as to indicate an IP address.

1.2.5 DNS Messages

All DNS messages use a single format:



The resolver sends the frame to the name server. Only the header and question section are used for the query. Replies or forwarding of the query use the same frame, but with more sections filled in (the answer/authority/additional sections).

1.2.5.1 Header format

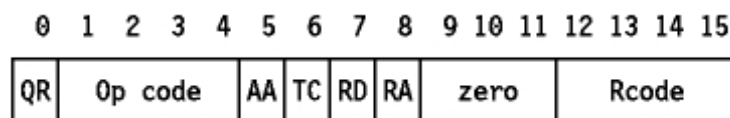
The header section, which is always present, has a fixed length of 12 bytes. The other sections are of variable length.

ID (Identification)

A 16-bit identifier assigned by the resolver. This identifier is copied in the corresponding reply from the name server and can be used to differentiate responses when multiple queries concur.

Parameters

A 16-bit field with the following format:



QR

Flag indicating a query (0) or a response (1).

Op code

4-bit field specifying the type of query:

- 0: standard query (QUERY)
- 1: inverse query (IQUERY)
- 2: server status request (STATUS)

Other values are reserved for future use.

AA

Authoritative Answer Flag. If this flag is set in a response, it indicates that the responding name server is an authority for the domain name sent in the query.

TC

Truncation Flag. This is set if the message is longer than permitted on the channel.

RD

Recursion desired flag. This bit tells the name server that recursive resolution is required. The bit is copied into the response.

RA

Recursion available flag. This indicates whether the name server supports recursive resolution.

zero

3 bits reserved for future use. Must be zero.

Rcode

4-bit response code. Possible values are:

- 0: No error condition.
- 1: Format error. The name server was unable to interpret the message.
- 2: Server failure. The message was not processed because of a problem with the name server.
- 3: Name error. The domain name in the query does not exist. This is only valid if the AA bit is set in the response.
- 4: Not implemented. The requested type of query is not implemented by the name server.
- 5: Refused. The name server refuses to respond for policy reasons.

Other values are reserved for future use.

QDcount

An unsigned 16-bit integer specifying the number of entries in the question section.

ANcount

An unsigned 16-bit integer specifying the number of RRs in the answer section.

NScount

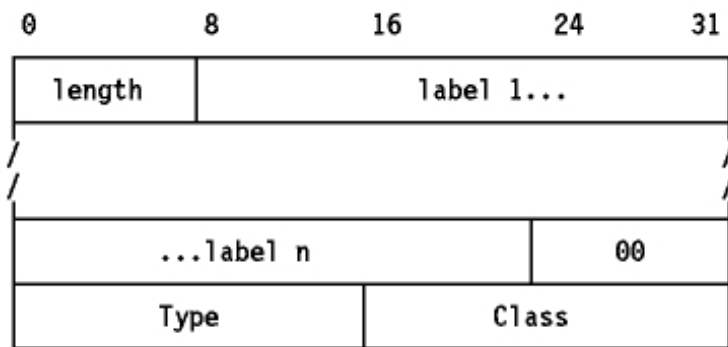
An unsigned 16-bit integer specifying the number of RRs in the authority section.

ARcount

An unsigned 16-bit integer specifying the number of RRs in the additional records section.

1.2.5.2 "Question" Section

The next section contains the queries for the name server. It contains Qdcount (usually 1) entries, each with the following format:



All of the fields are byte-aligned. The alignment of the “Type” field on a 4-byte boundary is included by way of example and is not required by the format.

length

A single byte giving the length of the next label.

label

A domain name element. The domain name is stored as a series of variable-length labels, each preceded by a “length” field.

00

00 indicates the end of the domain and represents the null label of the root domain.

Type

2 bytes specifying the query type. For address queries, this will be: ‘A’ (1) or ‘AAAA’ (28).

Class

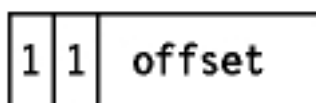
2 bytes specifying the query class. For Internet queries, this will be ‘IN’ (1).

1.2.5.3 "Answer", "Authority" and "Additional Resource" Sections

These three sections contain a variable number of resource records. The number is specified in the corresponding field of the header. The format of the resource records is discussed in section 2.3.

1.2.5.4 Message compression

In order to reduce the message size, a compression scheme is used to eliminate the repetition of domain names in the various RRs. Any duplicate domain name or list of labels is replaced with a pointer to the previous occurrence. The pointer has the form of a 2-byte field:



The first 2 bits distinguish the pointer from a normal label, which is restricted to a 63-byte length plus the length byte.

The ‘offset’ field specifies an offset from the start of the message. A zero offset specifies the first byte of the ID field in the header.

1.2.5.5 Transport

DNS messages are transmitted either as datagrams (UDP) or via a channel (TCP). In both cases, the destination port for DNS queries is port 53 (server source port).

A DNS resolver or server that sends a non-zone-transfer query *must* send a UDP query first. If the ‘answer’ section of the response is truncated and the requester supports TCP, it should try the query again using TCP. UDP is pre-

ferred over TCP for queries because UDP queries have a lower overhead and its use is essential for a heavily loaded server. Message truncation is not usually a problem given the current contents of the DNS database (typically 15 records can be sent in a datagram). However, this may change as new record types are added to the DNS.

TCP must be used for zone transfers because the 512-byte UDP limit will always be insufficient for a zone transfer.

Name servers must support both types of transport.

1.3 References

RFC 1034

DOMAIN NAMES – CONCEPTS AND FACILITIES, P. Mockapetris, November 1987

RFC 1035

DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, P. Mockapetris, November 1987

Chapter 2 Configuring DNS

2.1 Configuring DNS

To configure the DNS parameters, enter the *FEATURE DNS* command from the configuration menu.

```
*config

Config>feature dns

-- DNS resolver user configuration --
DNS config>
```

The options of this configuration menu are:

```
DNS config>?
cache           DNS Cache configuration
list            Displays the DNS configuration
n-retransmissions Maximum number of DNS query transmissions
no              Negates a command or sets its defaults
permanent-entry DNS permanent entry
probe           Adds url to a DNS probe
resolver-port   Listening port for external DNS queries
server          DNS name server
server-port     Destination port for DNS queries
servers-checking Checks access to DNS servers before request
source-address  Source address for DNS queries
t-retransmissions Time between DNS query retransmissions
exit
```



Note

The DNS service is not enabled by default. To activate it, at least one server or one permanent-entry must be configured. If no servers and no permanent-entries are configured, the service stops.

For more information, please see the sections on the *server* and *permanent-entry* commands.

2.1.1 CACHE

Configures the DNS cache. If this is enabled, each time the DNS server resolves a query and sends an answer, an entry (which includes the data obtained) is added to the cache. This ensures that clients don't repeatedly query the DNS server for the same address, as the cache is first checked to see if the answer is already there. The entry remains in the cache for the *time-to-live* (TTL) period specified in the TTL field.

```
DNS config>cache ?
default    Enables DNS cache with default configuration
size       DNS cache size in bytes
enable     Enables DNS cache
DNS config>
```

2.1.1.1 CACHE DEFAULT

Enables the DNS cache with the default values.

2.1.1.2 CACHE SIZE

Sets the size (in bytes) of the the DNS cache. Values allowed range from 100 bytes to 128 KB (131072 bytes). By default, the cache size is 10 KB (10240 bytes).

```
DNS config> cache size ?
<100..131072>    Cache size in bytes
DNS config>cache size 5000
DNS config>
```

2.1.1.3 CACHE ENABLE

Enables the DNS cache.

2.1.2 LIST

Displays the DNS configuration.

```
DNS config>list ?

all                Displays all the DNS configuration
cache              Displays the cache configuration
n-retransmissions  Displays the maximum number of retransmissions
permanent-entries Displays the configured DNS permanent entries
ports              Displays the ports used by DNS
probes             Displays the configured DNS probes
servers            Displays the configured DNS servers
servers-checking   Displays the configured DNS servers checking option
source-address     Displays the configured ip source address for DNS
queries
t-retransmissions  Displays the time between DNS query retransmissions
DNS config>
```

2.1.2.1 LIST ALL

Displays all DNS configuration information.

```
DNS config>list all
Source IPv4 address: 10.1.1.1
Source IPv4 address: 20.1.1.1, VRF=vrf-2
Source IPv6 address: 1234::1111
Resolver port: 53
Server port: 53
Number of retransmissions: 5
Time between retransmissions: 1 sec
Name servers:
172.24.0.6
172.24.0.13
1111::1234
Severs checking: disabled
Permanent entries:
    sip.teldat.es  type A 172.24.78.156
    cnmtest.com   type AAAA 1234::1119
Cache enabled
Cache size: 10240 bytes
Identifier: 1
    url: www.teldat.es
    url: www.google.com
DNS config>
```

<i>"Source IPv4 address"</i>	Source IPv4 address from which DNS queries are sent.
<i>"Source IPv6 address"</i>	Source IPv6 address from which DNS queries are sent.
<i>"Resolver port"</i>	DNS listening port that listens for DNS queries from external clients. The port listens for both UDP and TCP queries.
<i>"Server port"</i>	Destination port for DNS queries.
<i>"Number of retransmissions"</i>	Maximum number of DNS query transmissions.
<i>"Time between retransmissions"</i>	DNS query retransmission interval.
<i>"Name servers"</i>	IP addresses of the DNS servers configured.

<i>“Servers Checking”</i>	Configured DNS server checking option.
<i>“Permanent entries”</i>	Permanent DNS cache entries.
<i>“Cache enabled/disabled”</i>	DNS cache status.
<i>“Cache size”</i>	Maximum DNS cache size.
<i>“Identifier”</i>	Configured DNS probes.

Command history:

Release	Modification
10.09.31	This command shows VRF source-address information as of version 10.09.31.
11.00.07	This command shows VRF source-address information as of version 11.00.07.
11.01.05	This command shows VRF source-address information as of version 11.01.05.
11.01.07	This command shows the following new information as of version 11.01.07: - IPv6 source address - IPv6 server address - Type AAAA permanent-entries

2.1.2.2 LIST CACHE

Displays the current DNS cache status (enabled/disabled) and size (in bytes).

```
DNS config>list cache
Cache enabled
Cache size: 10240 bytes
DNS config>
```

2.1.2.3 LIST N-RETRANSMISSIONS

Displays the maximum number of DNS query transmissions.

```
DNS config>list n-retransmissions
Number of retransmissions: 5
DNS config>
```

2.1.2.4 LIST PERMANENT-ENTRIES

Displays the permanent entries in the DNS cache.

```
DNS config>list permanent-entries
Permanent entries:
      sip.teldat.es  type A  172.24.78.156
      cnmtest.com   type AAAA 1234::1119
DNS config>
```

Command history:

Release	Modification
11.01.07	This command shows AAAA permanent-entries as of version 11.01.07.

2.1.2.5 LIST PORTS

Displays the configured DNS ports: DNS listening port and DNS destination port.

```
DNS config>list ports
Resolver port: 53
Server port: 53
DNS config>
```

2.1.2.6 LIST PROBES

Displays the DNS probes configured.

```
DNS config>list probes
Identifier: 1
    url: www.teldat.es
    url: www.google.com
Identifier: 2
    url: www.hotmail.com
    url: www.yahoo.com
    url: www.amazon.com
DNS config>
```

2.1.2.7 LIST SERVERS

Displays the DNS server IP addresses configured.

```
DNS config>list servers
Name servers:
172.24.0.6
172.24.0.13
1234::1119
DNS config>
```

Command history:

Release	Modification
11.01.07	This command shows information on the IPv6 server address as of version 11.01.07.

2.1.2.8 LIST SERVERS-CHECKING

Displays the DNS server checking option configured.

```
DNS config>list servers-checking
Severs checking: enabled
DNS config>
```

2.1.2.9 LIST SOURCE-ADDRESS

Displays the DNS query source IP address.

```
DNS config>list source-address
Source IPv4 address: 10.1.1.1
Source IPv4 address: 20.1.1.1, VRF=vrf-2
Source IPv6 address: 1234::1111
DNS config>
```

Command history:

Release	Modification
10.09.31	This command shows VRF source-address information as of version 10.09.31.
11.00.07	This command shows VRF source-address information as of version 11.00.07.
11.01.05	This command shows VRF source-address information as of version 11.01.05.
11.01.07	This command shows IPv4/IPv6 source address information as of version 11.01.07.

2.1.2.10 LIST T-RETRANSMISSIONS

Displays the DNS query retransmission interval.

```
DNS config>list t-retransmissions
Time between retransmissions: 1 sec
DNS config>
```

2.1.3 N-RETRANSMISSIONS

Sets the maximum number of DNS query transmissions.

```
DNS config>n-retransmissions ?
<1..10>      Maximum number of retransmissions
DNS config>n-retransmissions 3
DNS config>
```

2.1.4 NO

Restores default values or deletes part of the configuration.

```
DNS config> no ?
cache          DNS Cache configuration
n-retransmissions  Maximum number of DNS query transmissions ns
permanent-entry  DNS permanent entry
probe          Adds url to a DNS probe
resolver-port    Listening port for external DNS queries
server          DNS name server
server-port      Destination port for DNS queries
servers-checking Checks access to DNS servers before request
source-address   Source address for DNS queries
t-retransmissions Time between DNS query retransmissions
DNS config>
```

2.1.4.1 NO CACHE ENABLE

Disables the cache.

2.1.4.2 NO CACHE SIZE

Returns the cache to its default size (10 KB).

2.1.4.3 NO N-RETRANSMISSIONS

Restores the maximum number of DNS query transmissions to the default setting (5).

2.1.4.4 NO PERMANENT-ENTRY

Deletes a permanent entry from the DNS cache. If you use NO PERMANENT-ENTRY [vrf<vrf_name>], all permanent entries with said URL are deleted. If you want to delete a specific entry, use NO PERMANENT-ENTRY with the following syntax:

Syntax:

```
DNS config>no permanent-entry [vrf <vrf_name>] <url> type {A | AAAA | SRV} <ipaddress> [ttl <ttl_val>]
```

<vrf_name> VRF associated with the cache containing the entry to be deleted.

<url> URL address.

<ipaddress> IP address corresponding to the URL (IPv4/IPv6).

<ttl_val> Cache entry TTL value.

Example:

```
DNS config>list permanent-entries
Permanent entries:
    sip.teldat.es  type A  172.24.78.156
    cnmtest.com   type AAAA 1234::1119
    www.colibri.es type A  171.11.12.13
    www.teldatp.es type A  172.24.23.23
    www.teldatp.es type A  172.24.23.24
    teldat_srv.es type SRV 1 255 5060 servidor.sip
    teldat_srv.es type SRV 2 255 5060 servidor2.sip
```

```

DNS config>no permanent-entry www.teldatp.es
DNS config>list permanent-entries
Permanent entries:
    sip.teldat.es  type A  172.24.78.156
    cnmtest.com   type AAAA 1234::1119
    www.colibri.es type A  171.11.12.13
    teldat_srv.es type SRV  1 255 5060 servidor.sip
    teldat_srv.es type SRV  2 255 5060 servidor2.sip
DNS config>no permanent-entry www.colibri.es type A  171.11.12.13
DNS config>list permanent-entries
Permanent entries:
    sip.teldat.es  type A  172.24.78.156
    cnmtest.com   type AAAA 1234::1119
    teldat_srv.es type SRV  1 255 5060 servidor.sip
    teldat_srv.es type SRV  2 255 5060 servidor2.sip
DNS config>no permanent-entry www.colibri.es
CLI Error: Permanent entry not found
CLI Error: Command error
DNS config>no permanent-entry teldat_srv.es type srv 2 255 5060 servidor2.sip
DNS config>list permanent-entries
Permanent entries:
    sip.teldat.es  type A  172.24.78.156
    cnmtest.com   type AAAA 1234::1119
    teldat_srv.es type SRV  1 255 5060 servidor.sip
DNS config>no permanent-entry cnmtest.com type AAAA 1234::1119
DNS config>list permanent-entries
Permanent entries:
    sip.teldat.es  type A  172.24.78.156
    teldat_srv.es type SRV  1 255 5060 servidor.sip

```

Command history:

Release	Modification
11.01.07	This command allows AAAA permanent-entries to be deleted as of version 11.01.07.

2.1.4.5 NO PROBE

Deletes a DNS probe or a ULR address included in a DNS probe. If you use no probe <id>, the DNS probe is completely deleted. If you use no probe <id> url <url>, a URL address included in the DNS probe is deleted.

```

DNS config>list probes
Identifier: 1
    url: www.teldat.es
    url: www.google.com
Identifier: 2
    url: www.hotmail.com
    url: www.yahoo.com
    url: www.amazon.com
DNS config>no probe 2 url www.yahoo.com
DNS config>list probes
Identifier: 1
    url: www.teldat.es
    url: www.google.com
Identifier: 2
    url: www.hotmail.com
    url: www.amazon.com
DNS config>no probe 1
DNS config>list probes
Identifier: 2
    url: www.hotmail.com
    url: www.amazon.com
DNS config>

```

2.1.4.6 NO RESOLVER-PORT

Sets the port used to listen for incoming DNS queries from external clients to its default value (port 53).

2.1.4.7 NO SERVER

Deletes a configured DNS name server.

```
DNS config>no server ?
  <a.b.c.d>      Name server IPv4 address to delete
  <a::b>         Name server IPv6 address to delete
  vrf           Specify a VPN routing and forwarding
DNS config>no server 192.68.63.56
DNS config>no server 1234::1119
DNS config>no server 1.2.3.4
CLI Error: Name server not found
CLI Error: Command error
DNS config>
```

Command history:

Release	Modification
11.01.07	This command allows an IPv6 server address to be deleted as of version 11.01.07.

2.1.4.8 NO SERVER-PORT

Returns the destination port for DNS queries to its default value (port 53).

2.1.4.9 NO SERVERS-CHECKING

Restores the DNS server checking option to its default value (disabled).

2.1.4.10 NO SOURCE-ADDRESS

Deletes the source IP address configured for the purpose of sending DNS queries. The device will go back to using the interface that the query came from as the source address.

```
DNS config>no source-address ?
  <a.b.c.d>      Source IPv4 address
  <a::b>         Source IPv6 address
  vrf           Specify a VPN routing and forwarding
DNS config>no source-address 10.1.1.1
DNS config>no source-address vrf vrf-2 20.1.1.1
DNS config>no source-address 30.1.1.1
CLI Error: Source address not found
CLI Error: Command error
DNS config>no source-address 1234::1111
DNS config>
```

Command history:

Release	Modification
11.01.07	This command allows an IPv6 source-address to be deleted as of version 11.01.07.

2.1.4.11 NO T-RETRANSMISSIONS

Restores the DNS query retransmission interval setting to its default value (1 second).

2.1.5 PERMANENT-ENTRY

Adds a permanent entry to the DNS cache. This can be an A entry, an AAAA entry or an SRV entry. You can create multiple entries for the same URL. Optionally, you can specify a *time to live* (TTL) value that is returned. The default TTL is 604800 seconds (7 days). Where a URL has multiple entries, and more than one entry has a TTL, the returned TTL value will be the largest of the specified values. The DNS service will start if there is at least one permanent-entry configured.

Syntax:

```
DNS config>permanent-entry [vrf <vrf_name>] <url> type {A | AAAA | SRV} <ipaddress> [ttl <ttl_val>]
```

<vrf_name> VRF associated with the cache the entry is going to be added to.

<code><url></code>	URL address.
<code><ipaddress></code>	IP address corresponding to the URL (IPv4/IPv6).
<code><tll_val></code>	TTL value of the cache entry.

Example:

```

DNS config>permanent-entry ?
<1..100 chars>    url
vrf                Specify a VPN routing and forwarding name
DNS config>permanent-entry www.teldatp.es ?
type              Type of the resource
DNS config>permanent-entry www.teldatp.es type ?
A                 Host IPv4 address
AAAA              Host IPv6 address
SRV               Service
DNS config>permanent-entry www.teldatp.es type A ?
<a.b.c.d>          IPv4 address
DNS config>permanent-entry www.teldatp.es type A 172.24.23.23
DNS config>
DNS config>permanent-entry www.teldatp.es type A 172.24.23.24
DNS config>
DNS config>permanent-entry cnmtest.com type AAAA ?
<a::b>            IPv6 address
DNS config>permanent-entry cnmtest.com type AAAA 1234::1119
DNS config>
DNS config>permanent-entry teldat_srv.es type SRV ?
<0..65535>        Priority
DNS config>permanent-entry teldat_srv.es type SRV 1 ?
<0..65535>        Weight
DNS config>permanent-entry teldat_srv.es type SRV 1 255 ?
<0..65535>        Port
DNS config>permanent-entry teldat_srv.es type SRV 1 255 5060 ?
<1..100 chars>    Target
DNS config>permanent-entry teldat_srv.es type SRV 1 255 5060 servidor.sip
DNS config>permanent-entry teldat_srv.es type SRV 2 255 5060 servidor2.sip ?
<cr>
ttl              Time to live returned (default 604800 sec)
DNS config>permanent-entry teldat_srv.es type SRV 2 255 5060 servidor2.sip ttl ?
<0..2146878847>   TTL in seconds
DNS config>permanent-entry teldat_srv.es type SRV 2 255 5060 servidor2.sip ttl 60
DNS config>
DNS config>permanent-entry teldat_srv.es type SRV 3 255 5060 servidor3.sip ttl 10
DNS config>

```

In this example, the TTL returned by teldat_srv.es is 60 seconds.

Command history:

Release	Modification
11.01.07	This command allows AAAA permanent-entries to be added as of version 11.01.07.

2.1.6 PROBE

Configures a DNS resolver probe. A DNS resolver probe is made up of a group of URLs. When you execute a probe from the monitoring menu, the device tries to resolve all the URLs that make up the probe at once. The time it takes to resolve the first URL is used to give an indication of the DNS resolution time.

```

DNS config>probe ?
<0..255>          DNS probe identifier
DNS config>probe 1 ?
url              URL to resolve
DNS config>probe 1 url ?
<1..100 chars>   Text
DNS config>

```

Example:

To create a DNS probe with the addresses `www.teldat.es`, `www.google.com` and `www.yahoo.com`, use the following commands:

```
DNS config>probe 1 url www.teldat.es
DNS config>probe 1 url www.google.com
DNS config>probe 1 url www.yahoo.com
DNS config>list probes
Identifier: 1
    url: www.teldat.es
    url: www.google.com
    url: www.yahoo.com
DNS config>
```

2.1.7 RESOLVER-PORT

Configures the port that listens for incoming DNS queries from external clients.

```
DNS config>resolver-port ?
<0..65535>    Resolver port
DNS config>resolver-port 10543
DNS config>
```

2.1.8 SERVER

Adds a DNS name server that can be used for DNS resolutions. The router acts as a DNS relay, forwarding DNS queries to the DNS servers added and sending their answers back to the clients. The router acts as an intermediary between the clients and the DNS servers. You can configure IPv4 and IPv6 servers. An error message is shown if you try to configure more servers than the maximum possible value (currently, you can configure three for each VRF. In secondary VRFs, only for servers that are not IPv6). The DNS service will start if there is at least one server configured.

Syntax:

```
DNS config>server [vrf <vrf_name>] <ipaddress>
```

<vrf_name> VRF used to communicate with the server.

<ipaddress> Server IP address (IPv4/IPv6).

Example:

```
DNS config>server ?
<a.b.c.d>    Name server IPv4 address
<a::b>      Name server IPv6 address
vrf         Specify a VPN routing and forwarding
DNS config>server 192.68.63.197
DNS config>server 172.24.0.7
DNS config>server 1234::1112
DNS config>server 192.168.212.3
CLI Error: Maximum number of name servers already configured
CLI Error: Command error
DNS config>server vrf ?
<word>      VPN routing and forwarding name
DNS config>server vrf vrf-2 172.16.0.34
DNS config>
```

Command history:

Release	Modification
11.01.07	This command allows IPv6 servers to be added as of version 11.01.07.

2.1.9 SERVER-PORT

Sets the destination port for DNS queries.

```
DNS config>server-port ?
```

```
<0..65535>    Server port
DNS config>server-port 342
DNS config>
```

2.1.10 SERVERS-CHECKING

Configures the DNS server checking option.

When this option is enabled, the device checks the access status of the configured servers. If they cannot be accessed, it responds to A-type queries with the IP address of the incoming interface for the query, and for the AAAA-type queries with the IPv6 link-local address of the incoming interface for the query.

If there is no configured or learned server, the device again responds with the IP address of the incoming interface for the query (please see the ipcp dns request for the PPP interface, Teldat-Dm710-I).

```
DNS config>servers-checking
DNS config>
```

2.1.11 SOURCE-ADDRESS

Sets the source address from which DNS queries are sent. You can configure one source address for each IP family (IPv4/IPv6). You can also specify one source-address for each secondary VRF, but only if the address is not IPv6.

```
DNS config>source-address ?
<a.b.c.d>    Source IPv4 address
<a::b>      Source IPv6 address
vrf         Specify a VPN routing and forwarding
DNS config>source-address 10.1.1.1
DNS config>source-address vrf vrf-2 20.1.1.1
DNS config>source-address 1234::1111
```

Command history:

Release	Modification
10.09.31	The VRF option was introduced on this command as of version 10.09.31.
11.00.07	The VRF option was introduced on this command as of version 11.00.07.
11.01.05	The VRF option was introduced on this command as of version 11.01.05.
11.01.07	The IPv6 source address option was introduced on this command as of version 11.01.07.

2.1.12 T-RETRANSMISSIONS

Configures the DNS query retransmission interval.

```
DNS config>t-retransmissions ?
<1s..10s>    Time between retransmissions (time value)
DNS config>t-retransmissions 5
DNS config>
```

2.1.13 EXIT

Exits the DNS configuration menu.

```
DNS config>exit
Config>
```

Chapter 3 Monitoring DNS

3.1 Monitoring DNS

To access the DNS monitoring menu, type **FEATURE DNS** at the global monitoring menu.

```
*monitor
Console Operator
+feature dns
-- DNS resolver user console --
DNS+
```

The options in the this monitoring menu are:

```
DNS+?
  cache      View the distinct DNS cache operating parameters
  list       Display the distinct DNS operating parameters
  lookup     Carry out a DNS petition for a specified name
  probe      Execute a DNS probe
  exit
DNS+
```

3.1.1 LIST

Displays various DNS operating parameters.

```
DNS+list ?
  lookup-results  Display the results of the last 10 DNS petitions
  memory-used     Display the memory resources in use for the DNS client
  probe          Show the DNS probe status
  servers         Displays active DNS servers
DNS+
```

3.1.1.1 LIST MEMORY-USED

Displays the memory resources that have been used for the DNS client.

```
DNS+list memory-used

Memory in use: 0
DNS+
```

Command history:

Release	Modification
11.01.08	The " <i>memory-used</i> " command was deleted as of version 11.01.08.

3.1.1.2 LIST LOOKUP-RESULTS

Displays the results of the last 10 DNS queries that have been carried out for monitoring purposes using the LOOKUP command.

Syntax:

```
DNS+list lookup-results [vrf <vrf_name>]
```

<vrf_name> VRF used by the LOOKUP command.

Example:

```
DNS+list lookup-results

Last DNS Lookup Queries
-----
www.elmundo.es: IP addresses
212.80.177.133
```

```
www.microsoft.com: Maximum number of retries reached
cnmtest.com: IP addresses
    1234::1119
DNS+
```

Command history:

Release	Modification
11.01.07	This command shows IPv6 address information as of version 11.01.07.

3.1.1.3 LIST PROBE

Displays the status of DNS probes.

```
DNS+list probe
Id      Status      URL              last      time
-----
  1    Completed OK    www.teldat.es 11/27/06 12:28:10 4
  2      Waiting              00/00/00 00:00:00 0
DNS+
```

The following fields are shown for each DNS probe:

"id"	DNS probe identifier.
"Status"	Probe status. This can be Waiting, Executed, Completed OK or Completed Error. A "Waiting" status is shown when a probe has never been executed, "Executed" is for a probe that is running, "Completed OK" is for a probe that has executed correctly and "Completed Error" is shown when a probe has executed but an error occurred that prevented DNS resolution for any of the URLs configured in the probe.
"URL"	First URL address to be resolved when the probe was last executed.
"last"	The date the probe was last executed. This field is filled with zeros if the probe hasn't been executed.
"time"	The time, in milliseconds, used in DNS probe resolution. The time shown corresponds to the time it takes to resolve the URL that returns the first answer (i.e., the first URL to be resolved).

3.1.1.4 LIST SERVERS

Displays the active DNS servers.

```
DNS+list servers
3 active servers found

Servers:
8.8.8.8
192.168.1.2
1234::1112
```

Command history:

Release	Modification
11.01.07	This command shows information on IPv6 servers as of version 11.01.07.

3.1.2 LOOKUP

Performs a DNS lookup for the specified name. You can specify the type of query: A or AAAA. (The default option is A-type)

The IP address retrieved from the DNS lookup operation appears on screen. The console is blocked during the lookup operation. To stop the DNS lookup operation, press Ctrl+C.

Syntax:

```
DNS+lookup [vrf <vrf_name>] name <url> [type {A | AAAA}]
```

<vrf_name>: VRF that should be used to make the request.

<url>: URL address to resolve.

Example:

```
DNS+lookup name www.teldat.es
Press Ctrl+C to stop the query

172.24.0.56
DNS+
DNS+lookup name cnmtest.com type AAAA
Press Ctrl+C to stop the query

1234::1119
```

If the query does not complete successfully, an error message indicating the type of error appears.

```
DNS+lookup name www.microsoft.com
Press Ctrl+C to stop the query

DNS Error: Maximum number of retries reached
DNS+
```

Command history:

Release	Modification
11.01.07	The type option was introduced on this command as of version 11.01.07.

3.1.3 CACHE

Allows you to display different DNS cache operation parameters, and to reset them.

```
DNS+cache ?
clear      Eliminate all entries in the DNS cache
find       Search for registers in the DNS cache
list       Display the entries the DNS cache contains
statistics Display a series of statistics parameters of the DNS cache
DNS+
```

3.1.3.1 CACHE CLEAR

Clears all entries from the DNS cache (except the permanent ones).

```
DNS+cache clear
DNS+
```

3.1.3.2 CACHE FIND

Allows you to search for cached DNS records. You can search for records by name or by record type. Make sure you enter the correct name/type, since wildcards are not accepted.

Syntax:

```
DNS+cache find name <url> [type <typename>] [vrf <vrf_name>]
DNS+cache find type <typename> [name <url>] [vrf <vrf_name>]
```

<url> Entry URL address.

<typename> Type of entry.

<vrf_name> VRF associated with the cache in which to search for the entry.

If you enter a record name and don't specify a type, all records that match that name are displayed, regardless of their type. In the same way, if you enter a record type without a name, all records for that type are displayed, regardless of the name they refer to.

Example: Enter the name you want to search for in the same line as the command. This searches for all record

types.

```
DNS+cache find name www.elmundo.es
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA

Entry Hash: 7388 Index: 0			
www.elmundo.es	A	0	193.110.128.200 193.110.128.209

```
DNS>cache find name www.google.es
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA

Entry Hash: 60 Index: 0			
www.google.es	CNAME	75305	www.google.com

DNS+

Example: Enter a name and type in the command line.

```
DNS+cache find name www.elmundo.es type a
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA

Entry Hash: 7388 Index: 0			
www.elmundo.es	A	0	193.110.128.200 193.110.128.209

DNS+

```
DNS+cache find name cnmtest.com type aaaa
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA

Entry Hash: 176 Index: 0			
cnmtest.com	AAAA	290	1234::1119

DNS+

Example: Search for all NS-type records.

```
DNS+cache find type ns
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA

Entry Hash: 5632 Index: 0			
elmundo.es	NS	24508	ns.el-mundo.net dns01.elmundo.es dns02.elmundo.es ineco.nic.es ns.elmundo.es
Entry Hash: 5800 Index: 0			
el-mundo.net	NS	82109	ns.el-mundo.net ns.elmundo.es ns.elmundo.org

DNS+

Example: Search for all records associated with a name, regardless of type.

```
DNS+cache find name elmundo.es
```

Cache entries found:

NAME	TYPE	TTL	RESOURCE RECORD DATA
------	------	-----	----------------------

```
-----
Entry Hash: 5632 Index: 0
  elmundo.es                NS      24320  ns.el-mundo.net
                             dns01.elmundo.es
                             dns02.elmundo.es
                             ineco.nic.es
                             ns.elmundo.es
DNS+
```

Command history:

Release	Modification
11.01.07	The AAAA type option was introduced on this command as of version 11.01.07.

The meaning of each cache element is explained in the section describing the **CACHE LIST** command. The following types can be searched for:

- “A”: address. IPv4 address associated with a name.
- “NS”: name server. Name of an authorized server for a name.
- “CNAME”: name alias.
- “PTR”: pointer to a domain name.
- “MX”: email exchange.
- “TXT”: text strings.
- “AAAA”: IP6 address. IPv6 address associated with a name.
- “SRV”: service.
- “ANY”: other types.

3.1.3.3 CACHE LIST

Displays the contents of the DNS cache. The cache can contain active and inactive (expired) entries. Active entries are entries that have not exceeded their *time to live* (TTL) value. Use the LIST command to display all entries, the active ones and the ones that have exceeded their TTL value.

Syntax:

```
DNS+cache list {active | all | expired} [vrf <vrf_name>]
```

<vrf_name> VRF associated with the cache.

CACHE LIST ACTIVE

Displays all cached entries that have not exceeded their TTL value and are, therefore, active.

```
DNS+cache list active

Cache Entries:

      NAME                TYPE      TTL      RESOURCE RECORD DATA
-----
Entry Hash: 76 Index: 0
  sip.teldat.es                A      INF  172.24.78.156
                             172.24.78.152

Entry Hash: 176 Index: 0
  cnmtest.com                AAAA      291  1234::1119

Entry Hash: 1304 Index: 2
  img.mediaplex.com.edgesuite.net  CNAME      8179  a1470.g.akamai.net

Entry Hash: 3440 Index: 0
  ns.elmundo.es                A      23386  193.110.128.201

Entry Hash: 3612 Index: 0
  ttd.cache.el-mundo.net        A        69  213.4.105.38
                             213.4.105.36
                             213.4.105.37

Entry Hash: 5632 Index: 0
  elmundo.es                NS      23380  ns.el-mundo.net
                             dns01.elmundo.es
                             dns02.elmundo.es
```

			ineco.nic.es
			ns.elmundo.es
Entry Hash: 5800 Index: 0			
el-mundo.net	NS	80981	ns.el-mundo.net
			ns.elmundo.es
			ns.elmundo.org
Entry Hash: 6896 Index: 0			
ineco.nic.es	A	2311	194.69.254.2
Entry Hash: 7028 Index: 0			
dns02.elmundo.es	A	23379	193.110.128.51
Entry Hash: 7800 Index: 0			
dns01.elmundo.es	A	23379	193.110.128.50
DNS+			

CACHE LIST ALL

Displays all cached entries, both active and expired.

DNS+cache list all			
Cache Entries:			
	NAME	TYPE	TTL RESOURCE RECORD DATA
	-----	-----	-----
Entry Hash: 20 Index: 0			
ad.snv.mediaplex.com	A	0	64.158.223.128
Entry Hash: 76 Index: 0			
sip.teldat.es	A	INF	172.24.78.156
			172.24.78.152
Entry Hash: 176 Index: 0			
cnmtest.com	AAAA	291	1234::1119
Entry Hash: 212 Index: 0			
gblx.cache.el-mundo.net	A	0	64.215.202.23
			64.215.202.21
			64.215.202.22
Entry Hash: 316 Index: 0			
estaticos.elmundo.es	CNAME	0	active.cache.el-mundo.NET
Entry Hash: 408 Index: 0			
ns2.mediaplex.com	A	0	64.70.10.79
Entry Hash: 1304 Index: 2			
img.mediaplex.com.edgesuite.net	CNAME	8179	a1470.g.akamai.net
Entry Hash: 1368 Index: 0			
elmundo.ojdinteractiva.com	A	0	193.110.128.55
Entry Hash: 3440 Index: 0			
ns.elmundo.es	A	23386	193.110.128.201
Entry Hash: 3612 Index: 0			
ttd.cache.el-mundo.net	A	69	213.4.105.38
			213.4.105.36
			213.4.105.37
Entry Hash: 5632 Index: 0			
elmundo.es	NS	23380	ns.el-mundo.net
			dns01.elmundo.es
			dns02.elmundo.es
			ineco.nic.es
			ns.elmundo.es
Entry Hash: 5800 Index: 0			
el-mundo.net	NS	80981	ns.el-mundo.net
			ns.elmundo.es
			ns.elmundo.org
Entry Hash: 6896 Index: 0			
ineco.nic.es	A	2311	194.69.254.2
Entry Hash: 7028 Index: 0			
dns02.elmundo.es	A	23379	193.110.128.51
Entry Hash: 7800 Index: 0			
dns01.elmundo.es	A	23379	193.110.128.50
DNS+			

CACHE LIST EXPIRED

Displays all cached entries that have exceeded their TTL value and are, therefore, no longer active.

```
DNS+cache list expired
```

Cache Entries:

NAME	TYPE	TTL	RESOURCE RECORD DATA
Entry Hash: 20 Index: 0			
ad.snv.mediaplex.com	A	0	64.158.223.128
Entry Hash: 176 Index: 0			
cnmtest.com	AAAA	0	1234::1119
Entry Hash: 212 Index: 0			
gblx.cache.el-mundo.net	A	0	64.215.202.23 64.215.202.21 64.215.202.22
Entry Hash: 316 Index: 0			
estaticos.elmundo.es	CNAME	0	active.cache.el-mundo.NET
Entry Hash: 408 Index: 0			
ns2.mediaplex.com	A	0	64.70.10.79
Entry Hash: 1368 Index: 0			
elmundo.ojdinteractiva.com	A	0	193.110.128.55

DNS+

The parameters displayed have the following meanings:

<i>Entry Hash:</i>	The entry's position in the search table (Hash).
<i>Index:</i>	Indicates the occurrence number for a Hash entry.
<i>NAME:</i>	DNS name associated with the entry.
<i>TYPE:</i>	Entry type. The meaning of the types is explained in the section on the CACHE FIND command.
<i>TTL:</i>	Time to Live (TTL). This is how much time is left before the cache entry expires. If this is INF (infinite), the entry is permanent.
<i>RESOURCE RECORD DATA:</i>	Saved DNS data for the name in this cache entry.

Command history:

Release	Modification
11.01.07	These commands show information on AAAA entries as of version 11.01.07.

3.1.3.4 CACHE STATISTICS

Displays a series of statistical parameters that can help obtain information about the state of the DNS cache and about the activity registered in said cache.

Syntax:

```
DNS+cache statistics [vrf <vrf_name>]
```

<vrf_name> VRF associated with the cache.

Example:

```
DNS+cache statistics

DNS cache statistics:

Cache status:.....ACTIVE
Cache received queries:.14
Cache motions:.....1701
```

```

UDP active queries:.....0
TCP active queries:.....0
Total cache entries.....32
Active cache entries....8
Expired cache entries...24
Cache rounds.....0
Type A entries.....17
Type NS entries.....1
Type CNAME entries.....11
Type PTR entries.....0
Type MX entries.....0
Type TXT entries.....0
Type AAAA entries.....2
Type SRV entries.....0
Type ANY entries.....1
Type unknown entries....0

```

DNS+

The parameters displayed have the following meanings:

<i>Cache status:</i>	Indicates whether the DNS cache is activated.
<i>Cache received queries:</i>	Number of DNS queries received from external devices.
<i>Cache motions:</i>	Number of Cache movements.
<i>UDP active queries:</i>	Active DNS queries, requested through UDP.
<i>TCP active queries:</i>	Active DNS queries, requested through TCP.
<i>Total cache entries:</i>	Total number of cache entries.
<i>Active cache entries:</i>	Number of active cache entries (TTL != 0).
<i>Expired cache entries:</i>	Number of inactive cache entries (TTL = 0).
<i>Cache rounds:</i>	Number of times the entire circular cache buffer has been traversed.
<i>Type A entries:</i>	Number of A cache entries.
<i>Type unknown entries:</i>	Number of NS cache entries.
<i>Type CNAME entries:</i>	Number of CNAME cache entries.
<i>Type PTR entries:</i>	Number of PTR cache entries.
<i>Type MX entries:</i>	Number of MX cache entries.
<i>Type TXT entries:</i>	Number of TXT cache entries.
<i>Type AAAA entries:</i>	Number of AAAA cache entries.
<i>Type SRV entries:</i>	Number of SRV cache entries.
<i>Type ANY entries:</i>	Number of ANY cache entries.
<i>Type unknown entries:</i>	Number of cache entries that are not one of the above.

Command history:

Release	Modification
11.01.07	This command shows information on AAAA entries as of version 11.01.07.

3.1.4 PROBE

Allows you to run a DNS probe.

```
DNS+probe ?
  close-start    Start a DNS probe (with PPP interface specified)
  start          Start a DNS probe
DNS+
```

3.1.4.1 PROBE START

Starts the specified DNS probe. When you run a DNS probe, the device sends out queries to resolve all the URLs that make up the DNS probe, saving the fastest URL resolution time. If the probe cannot be executed, an error message is shown.

```
DNS+probe start probe-id 1
DNS+probe start probe-id 3

DNS Error: Requested probe not found
DNS+
```

3.1.4.2 PROBE CLOSE-START

Starts the DNS probe specified. With this command the probe doesn't start straight off, unlike what happens with the **PROBE START** command. The DNS probe starts once you have specified a PPP interface (thus disconnecting it) and the connection is re-established. The PPP interface ID matches the interface index used in SNMP.

```
DNS+probe close-start probe-id 2 ppp-ifc 8
DNS+
```

3.1.5 EXIT

Exits the DNS client monitoring menu.

```
DNS+exit
+
```