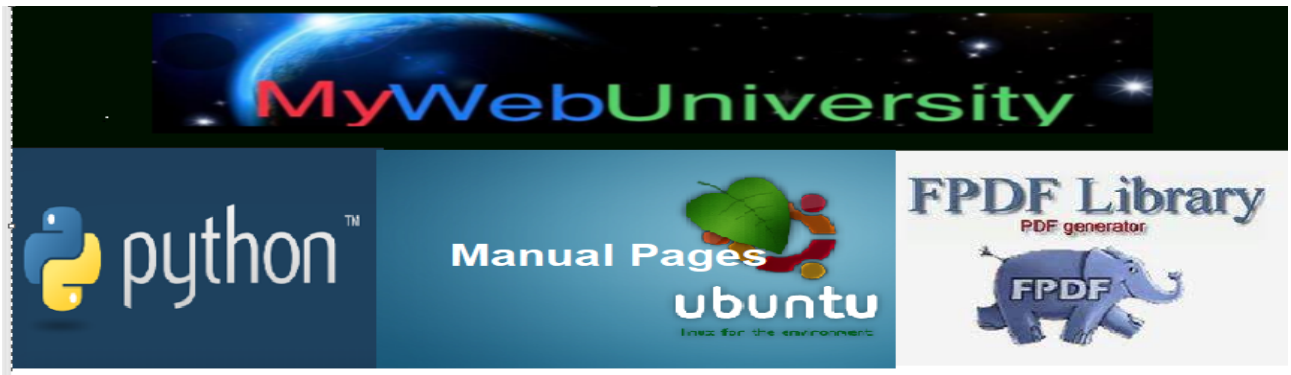


***Full credit is given to the above companies including the OS that this PDF file was generated!***

## *Linux Ubuntu 26.04 Manual Pages on command 'dig.1'*

***$ man dig.1***

DIG(1) BIND 9 DIG(1)

NAME

dig - DNS lookup utility

SYNOPSIS

dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-v] [-x addr] [-y [hmac:]name:key] [ [-4] | [-6] ] [name] [type] [class] [query? opt...]

dig [-h]

dig [global-queryopt...] [query...]

DESCRIPTION

dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and dis? plays the answers that are returned from the name server(s) that were queried. Most DNS ad? ministrators use dig to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. Other lookup tools tend to have less functionality than dig.

Although dig is normally used with command-line arguments, it also has a batch mode of oper? ation for reading lookup requests from a file. A brief summary of its command-line arguments and options is printed when the -h option is given. The BIND 9 implementation of dig allows multiple lookups to be issued from the command line.

Unless it is told to query a specific name server, dig tries each of the servers listed in /etc/resolv.conf. If no usable server addresses are found, dig sends the query to the local host.

When no command-line arguments or options are given, dig performs an NS query for "." (the root).

It is possible to set per-user defaults for dig via ${HOME}/.digrc. This file is read and any options in it are applied before the command-line arguments. The -r option disables this feature, for scripts that need predictable behavior.

The IN and CH class names overlap with the IN and CH top-level domain names. Either use the -t and -c options to specify the type and class, use the -q to specify the domain name, or use "IN." and "CH." when looking up these top-level domains.

## SIMPLE USAGE

A typical invocation of dig looks like:

```
dig @server name type
```

where:

server is the name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-delimited notation. When the supplied server argument is a hostname, dig resolves that name before querying that name server.

If no server argument is provided, dig consults /etc/resolv.conf; if an address is found there, it queries the name server at that address. If either of the -4 or -6 options are in use, then only addresses for the corresponding transport are tried. If no usable addresses are found, dig sends the query to the local host. The reply from the name server that responds is displayed.

name is the name of the resource record that is to be looked up.

type indicates what type of query is required - ANY, A, MX, SIG, etc. type can be any valid query type. If no type argument is supplied, dig performs a lookup for an A record.

## OPTIONS

-4 This option indicates that only IPv4 should be used.

-6 This option indicates that only IPv6 should be used.

-b address[#port]

This option sets the source IP address of the query. The address must be a valid address on one of the host's network interfaces, or "0.0.0.0" or "::". An optional port may be specified by appending #port.

-c class

This option sets the query class. The default class is IN; other classes are HS for Hesiod records or CH for Chaosnet records.

-f file

This option sets batch mode, in which dig reads a list of lookup requests to process from the given file. Each line in the file should be organized in the same way it would be presented as a query to dig using the command-line interface.

-h Print a usage summary.

-k keyfile

This option tells dig to sign queries using TSIG or SIG(0) using a key read from the given file. Key files can be generated using tsig-keygen <#std-iscman-tsig-keygen>. When using TSIG authentication with dig, the name server that is queried needs to know the key and algorithm that is being used. In BIND, this is done by providing ap? propriate key and server statements in named.conf <#std-iscman-named.conf> for TSIG and by looking up the KEY record in zone data for SIG(0).

-m This option enables memory usage debugging.

-p port

This option sends the query to a non-standard port on the server, instead of the de? fault port 53. This option is used to test a name server that has been configured to listen for queries on a non-standard port number.

-q name

This option specifies the domain name to query. This is useful to distinguish the name from other arguments.

-r This option indicates that options from ${HOME}/.digrc should not be read. This is useful for scripts that need predictable behavior.

-t type

This option indicates the resource record type to query, which can be any valid query type. If it is a resource record type supported in BIND 9, it can be given by the type mnemonic (such as NS or AAAA). The default query type is A, unless the -x option is supplied to indicate a reverse lookup. A zone transfer can be requested by speci? fying a type of AXFR. When an incremental zone transfer (IXFR) is required, set the type to ixfr=N. The incremental zone transfer contains all changes made to the zone since the serial number in the zone's SOA record was N.

All resource record types can be expressed as TYPEnn, where nn is the number of the type. If the resource record type is not supported in BIND 9, the result is displayed as described in RFC 3597 <https://datatracker.ietf.org/doc/html/rfc3597.html>.

-u This option indicates that print query times should be provided in microseconds in? stead of milliseconds.

-v This option prints the version number and exits.

-x addr

This option sets simplified reverse lookups, for mapping addresses to names. The addr is an IPv4 address in dotted-decimal notation, or a colon-delimited IPv6 address. When the -x option is used, there is no need to provide the name, class, and type ar? guments. dig automatically performs a lookup for a name like 94.2.0.192.in-addr.arpa and sets the query type and class to PTR and IN respectively. IPv6 addresses are looked up using nibble format under the IP6.ARPA domain.

-y [hmac:]keyname:secret

This option signs queries using TSIG with the given authentication key. keyname is the name of the key, and secret is the base64-encoded shared secret. hmac is the name of the key algorithm; valid choices are hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384, or hmac-sha512. If hmac is not specified, the default is hmac-md5; if MD5 was disabled, the default is hmac-sha256.

Note:

Only the -k option should be used, rather than the -y option, because with -y the shared secret is supplied as a command-line argument in clear text. This may be visible in the output from ps1 or in a history file maintained by the user's shell.

QUERY OPTIONS

dig provides a number of query options which affect the way in which lookups are made and the results displayed. Some of these set or reset flag bits in the query header, some deter? mine which sections of the answer get printed, and others determine the timeout and retry strategies.

Each query option is identified by a keyword preceded by a plus sign (+). Some keywords set or reset an option; these may be preceded by the string no to negate the meaning of that keyword. Other keywords assign values to options, like the timeout interval. They have the form +keyword=value. Keywords may be abbreviated, provided the abbreviation is unambiguous; for example, +cd is equivalent to +cdflag. The query options are:

+aaflag, +noaaflag

This option is a synonym for +aaonly, +noaaonly.

+aaonly, +noaaonly

This option sets the aa flag in the query.

+additional, +noadditional

This option displays [or does not display] the additional section of a reply. The de? fault is to display it.

+adflag, +noadflag

This option sets [or does not set] the AD (authentic data) bit in the query. This re? quests the server to return whether all of the answer and authority sections have been validated as secure, according to the security policy of the server. AD=1 indi? cates that all records have been validated as secure and the answer is not from a OPT-OUT range. AD=0 indicates that some part of the answer was insecure or not vali? dated. This bit is set by default.

+all, +noall

This option sets or clears all display flags.

+answer, +noanswer

This option displays [or does not display] the answer section of a reply. The default is to display it.

+authority, +noauthority

This option displays [or does not display] the authority section of a reply. The de? fault is to display it.

+badcookie, +nobadcookie

This option retries the lookup with a new server cookie if a BADCOOKIE response is received.

+besteffort, +nobesteffort

This option attempts to display the contents of messages which are malformed. The de? fault is to not display malformed answers.

+bufsize[=B]

This option sets the UDP message buffer size advertised using EDNS0 to B bytes. The maximum and minimum sizes of this buffer are 65535 and 0, respectively. +bufsize re? stores the default buffer size.

+cd, +cdflag, +nocdflag

This option sets [or does not set] the CD (checking disabled) bit in the query. This requests the server to not perform DNSSEC validation of responses.

+class, +noclass

This option displays [or does not display] the CLASS when printing the record.

+cmd, +nocmd

This option toggles the printing of the initial comment in the output, identifying the version of dig and the query options that have been applied. This option always has a global effect; it cannot be set globally and then overridden on a per-lookup basis. The default is to print this comment.

+coflag, +co, +nocoflag, +noco

This option sets [or does not set] the CO (Compact denial of existence Ok) EDNS bit in the query. If set, it tells servers that Compact Denial of Existence responses are acceptable when replying to queries. The default is +nocoflag.

+comments, +nocomments

This option toggles the display of some comment lines in the output, with information about the packet header and OPT pseudosection, and the names of the response section.

The default is to print these comments.

Other types of comments in the output are not affected by this option, but can be controlled using other command-line switches. These include +cmd, +question, +stats, and +rrcomments.

+cookie=####, +nocookie

This option sends [or does not send] a COOKIE EDNS option, with an optional value. Replaying a COOKIE from a previous response allows the server to identify a previous client. The default is +cookie.

+cookie is also set when +trace is set to better emulate the default queries from a nameserver.

+crypto, +nocrypto

This option toggles the display of cryptographic fields in DNSSEC records. The con? tents of these fields are unnecessary for debugging most DNSSEC validation failures and removing them makes it easier to see the common failures. The default is to dis? play the fields. When omitted, they are replaced by the string [omitted] or, in the DNSKEY case, the key ID is displayed as the replacement, e.g. [ key id = value ].

+defname, +nodefname

This option, which is deprecated, is treated as a synonym for +search, +nosearch.

+dns64prefix, +nodns64prefix

Lookup IPV4ONLY.ARPA AAAA and print any DNS64 prefixes found.

+dnssec, +do, +nodnssec, +nodo

This option requests that DNSSEC records be sent by setting the DNSSEC OK (DO) bit in the OPT record in the additional section of the query.

+domain=somename

This option sets the search list to contain the single domain somename, as if speci? fied in a domain directive in /etc/resolv.conf, and enables search list processing as if the +search option were given.

+edns[=#], +noedns

This option specifies the EDNS version to query with. Valid values are 0 to 255. Setting the EDNS version causes an EDNS query to be sent. +noedns clears the remem? bered EDNS version. EDNS is set to 0 by default.

+ednsflags[=#], +noednsflags

This option sets the must-be-zero EDNS flags bits (Z bits) to the specified value. Decimal, hex, and octal encodings are accepted. Setting a named flag (e.g. DO, CO) is silently ignored. By default, no Z bits are set.

+ednsnegotiation, +noednsnegotiation

This option enables/disables EDNS version negotiation. By default, EDNS version nego? tiation is enabled.

+ednsopt[=code[:value]], +noednsopt

This option specifies the EDNS option with code point code and an optional payload of value as a hexadecimal string. code can be either an EDNS option name (for example, NSID or ECS) or an arbitrary numeric value. +noednsopt clears the EDNS options to be sent.

+expire, +noexpire

This option sends an EDNS Expire option.

+fail, +nofail

This option indicates that named <#std-iscman-named> should try [or not try] the next server if a SERVFAIL is received. The default is to not try the next server, which is the reverse of normal stub resolver behavior.

+fuzztime[=value], +nofuzztime

This option allows the signing time to be specified when generating signed messages. If a value is specified it is the seconds since 00:00:00 January 1, 1970 UTC ignoring leap seconds. If no value is specified 1646972129 (Fri 11 Mar 2022 04:15:29 UTC) is

used. The default is +nofuzztime and the current time is used.

+header-only, +noheader-only

This option sends a query with a DNS header without a question section. The default is to add a question section. The query type and query name are ignored when this is set.

+https[=value], +nohttps

This option indicates whether to use DNS over HTTPS (DoH) when querying name servers. When this option is in use, the port number defaults to 443. The HTTP POST request mode is used when sending the query.

If value is specified, it will be used as the HTTP endpoint in the query URI; the de? fault is /dns-query. So, for example, dig @example.com +https will use the URI https://example.com/dns-query.

+https-get[=value], +nohttps-get

Similar to +https, except that the HTTP GET request mode is used when sending the query.

+https-post[=value], +nohttps-post

Same as +https.

+http-plain[=value], +nohttp-plain

Similar to +https, except that HTTP queries will be sent over a non-encrypted chan? nel. When this option is in use, the port number defaults to 80 and the HTTP request mode is POST.

+http-plain-get[=value], +nohttp-plain-get

Similar to +http-plain, except that the HTTP request mode is GET.

+http-plain-post[=value], +nohttp-plain-post

Same as +http-plain.

+identify, +noidentify

This option shows [or does not show] the IP address and port number that supplied the answer, when the +short option is enabled. If short form answers are requested, the default is not to show the source address and port number of the server that provided the answer.

+idn, +noidn

Enable or disable IDN processing. By default IDN is enabled for input query names, and for display when the output is a terminal.

You can also turn off dig's IDN processing by setting the IDN_DISABLE environment variable.

+ignore, +noignore

This option ignores [or does not ignore] truncation in UDP responses instead of retrying with TCP. By default, TCP retries are performed.

+keepalive, +nokeepalive

This option sends [or does not send] an EDNS Keepalive option.

+keepopen, +nokeepopen

This option keeps [or does not keep] the TCP socket open between queries, and reuses it rather than creating a new TCP socket for each lookup. The default is +nokeepopen.

+multiline, +nomultiline

This option prints [or does not print] records, like the SOA records, in a verbose multi-line format with human-readable comments. The default is to print each record on a single line to facilitate machine parsing of the dig output.

+ndots=D

This option sets the number of dots (D) that must appear in name for it to be consid? ered absolute. The default value is that defined using the ndots statement in /etc/resolv.conf, or 1 if no ndots statement is present. Names with fewer dots are interpreted as relative names, and are searched for in the domains listed in the search or domain directive in /etc/resolv.conf if +search is set.

+nsid, +nonsid

When enabled, this option includes an EDNS name server ID request when sending a query.

+nssearch, +nonssearch

When this option is set, dig attempts to find the authoritative name servers for the zone containing the name being looked up, and display the SOA record that each name server has for the zone. Addresses of servers that did not respond are also printed.

+onesoa, +noonesoa

When enabled, this option prints only one (starting) SOA record when performing an AXFR. The default is to print both the starting and ending SOA records.

+opcode=value, +noopcode

When enabled, this option sets (restores) the DNS message opcode to the specified value. The default value is QUERY (0).

+padding=value

This option pads the size of the query packet using the EDNS Padding option to blocks of value bytes. For example, +padding=32 causes a 48-byte query to be padded to 64 bytes. The default block size is 0, which disables padding; the maximum is 512. Val? ues are ordinarily expected to be powers of two, such as 128; however, this is not mandatory. Responses to padded queries may also be padded, but only if the query uses TCP or DNS COOKIE.

+proxy[=src_addr[#src_port]-dst_addr[#dst_port]], +noproxy

When this option is set, dig adds PROXYv2 headers to the queries. When source and destination addresses are specified, the headers contain them and use the PROXY com? mand. It means for the remote peer that the queries were sent on behalf of another node and that the PROXYv2 header reflects the original connection endpoints. The de? fault source port is 0 and destination port is 53.

For encrypted DNS transports, to prevent accidental information leakage, encryption is applied to the PROXYv2 headers: the headers are sent right after the handshake process has been completed.

For plain DNS transports, no encryption is applied to the PROXYv2 headers.

If the addressees are omitted, PROXYv2 headers, that use the LOCAL command set, are added instead. For the remote peer, that means that the queries were sent on purpose without being relayed, so the real connection endpoint addresses must be used.

+proxy-plain[=src_addr[#src_port]-dst_addr[#dst_port], +noproxy-plain

The same as +[no]proxy, but instructs dig to send PROXYv2 headers ahead of any en? cryption, before any handshake messages are sent. That makes dig behave exactly how it is described in the PROXY protocol specification, but not all software expects such behaviour.

Please consult the software documentation to find out if you need this option. (for example, dnsdist expects encrypted PROXYv2 headers sent over TLS when encryption is used, while HAProxy and many other software packages expect plain ones).

For plain DNS transports the option is effectively an alias for the +[no]proxy de? scribed above.

+qid=value

This option specifies the query ID to use when sending queries.

+qr, +noqr

This option toggles the display of the query message as it is sent. By default, the query is not printed.

+question, +noquestion

This option toggles the display of the question section of a query when an answer is returned. The default is to print the question section as a comment.

+raflag, +noraflag

This option sets [or does not set] the RA (Recursion Available) bit in the query. The default is +noraflag. This bit is ignored by the server for QUERY.

+rdflag, +nordflag

This option is a synonym for +recurse, +norecurse.

+recurse, +norecurse

This option toggles the setting of the RD (recursion desired) bit in the query. This bit is set by default, which means dig normally sends recursive queries. Recursion is automatically disabled when the +nssearch or +trace query option is used.

+retry=T

This option sets the number of times to retry UDP and TCP queries to server to T in? stead of the default, 2. Unlike +tries, this does not include the initial query.

+rrcomments, +norrcomments

This option toggles the display of per-record comments in the output (for example, human-readable key information about DNSKEY records). The default is not to print record comments unless multiline mode is active.

+search, +nosearch

This option uses [or does not use] the search list defined by the searchlist or do? main directive in resolv.conf, if any. The search list is not used by default.
ndots from resolv.conf (default 1), which may be overridden by +ndots, determines whether the name is treated as relative and hence whether a search is eventually per? formed.

+short, +noshort

This option toggles whether a terse answer is provided. The default is to print the answer in a verbose form. This option always has a global effect; it cannot be set globally and then overridden on a per-lookup basis.

+showbadcookie, +noshowbadcookie

This option toggles whether to show the message containing the BADCOOKIE rcode before

retrying the request or not. The default is to not show the messages.

+showbadvers, +noshowbadvers

This option toggles whether to show the message containing the BADVERS rcode before retrying the request or not. The default is to not show the messages.

+showsearch, +noshowsearch

This option performs [or does not perform] a search showing intermediate results.

+split=W

This option splits long hex- or base64-formatted fields in resource records into chunks of W characters (where W is rounded up to the nearest multiple of 4). +nosplit or +split=0 causes fields not to be split at all. The default is 56 characters, or 44 characters when multiline mode is active.

+stats, +nostats

This option toggles the printing of statistics: when the query was made, the size of the reply, etc. The default behavior is to print the query statistics as a comment after each lookup.

+subnet=addr[/prefix-length], +nosubnet

This option sends [or does not send] an EDNS CLIENT-SUBNET option with the specified IP address or network prefix.

dig +subnet=0.0.0.0/0, or simply dig +subnet=0 for short, sends an EDNS CLIENT-SUBNET option with an empty address and a source prefix-length of zero, which signals a re? solver that the client's address information must not be used when resolving this query.

+tcflag, +notcflag

This option sets [or does not set] the TC (TrunCation) bit in the query. The default is +notcflag. This bit is ignored by the server for QUERY.

+tcp, +notcp

This option indicates whether to use TCP when querying name servers. The default be? havior is to use UDP unless a type any or ixfr=N query is requested, in which case the default is TCP. AXFR queries always use TCP. To prevent retry over TCP when TC=1 is returned from a UDP query, use +ignore.

+timeout=T

This option sets the timeout for a query to T seconds. The default timeout is 5 sec? onds. An attempt to set T to less than 1 is silently set to 1.

+tls, +notls

This option indicates whether to use DNS over TLS (DoT) when querying name servers. When this option is in use, the port number defaults to 853.

+tls-ca[=file-name], +notls-ca

This option enables remote server TLS certificate validation for DNS transports, relying on TLS. Certificate authorities certificates are loaded from the specified PEM file (file-name). If the file is not specified, the default certificates from the global certificates store are used.

+tls-certfile=file-name, +tls-keyfile=file-name, +notls-certfile, +notls-keyfile

These options set the state of certificate-based client authentication for DNS transports, relying on TLS. Both certificate chain file and private key file are expected to be in PEM format. Both options must be specified at the same time.

+tls-hostname=hostname, +notls-hostname

This option makes dig use the provided hostname during remote server TLS certificate verification. Otherwise, the DNS server name is used. This option has no effect if +tls-ca is not specified.

+trace, +notrace

This option toggles tracing of the delegation path from the root name servers for the name being looked up. Tracing is disabled by default. When tracing is enabled, dig makes iterative queries to resolve the name being looked up. It follows referrals from the root servers, showing the answer from each server that was used to resolve the lookup.

If @server is also specified, it affects only the initial query for the root zone name servers.

+dnssec is set when +trace is set, to better emulate the default queries from a name server.

Note that the delv +ns option can also be used for tracing the resolution of a name from the root (see delv <#std-iscman-delv>).

+tries=T

This option sets the number of times to try UDP and TCP queries to server to T instead of the default, 3. If T is less than or equal to zero, the number of tries is silently rounded up to 1.

+ttlid, +nottlid

This option displays [or does not display] the TTL when printing the record.

+ttlunits, +nottlunits

This option displays [or does not display] the TTL in friendly human-readable time units of s, m, h, d, and w, representing seconds, minutes, hours, days, and weeks. This implies +ttlid.

+unknownformat, +nounknownformat

This option prints all RDATA in unknown RR type presentation format (RFC 3597 <https://datatracker.ietf.org/doc/html/rfc3597.html>). The default is to print RDATA for known types in the type's presentation format.

+vc, +novc

This option uses [or does not use] TCP when querying name servers. This alternate syntax to +tcp is provided for backwards compatibility. The vc stands for "virtual circuit."

+yaml, +noyaml

When enabled, this option prints the responses (and, if +qr is in use, also the out? going queries) in a detailed YAML format.

+zflag, +nozflag

This option sets [or does not set] the last unassigned DNS header flag in a DNS query. This flag is off by default.

MULTIPLE QUERIES

The BIND 9 implementation of dig supports specifying multiple queries on the command line (in addition to supporting the -f batch file option). Each of those queries can be supplied with its own set of flags, options, and query options.

In this case, each query argument represents an individual query in the command-line syntax described above. Each consists of any of the standard options and flags, the name to be looked up, an optional query type and class, and any query options that should be applied to that query.

A global set of query options, which should be applied to all queries, can also be supplied. These global query options must precede the first tuple of name, class, type, options, flags, and query options supplied on the command line. Any global query options (except +cmd and +short options) can be overridden by a query-specific set of query options. For example:

```
dig +qr www.isc.org any -x 127.0.0.1 isc.org ns +noqr
```

shows how dig can be used from the command line to make three lookups: an ANY query for

www.isc.org, a reverse lookup of 127.0.0.1, and a query for the NS records of isc.org. A global query option of +qr is applied, so that dig shows the initial query it made for each lookup. The final query has a local query option of +noqr which means that dig does not print the initial query when it looks up the NS records for isc.org.

## RETURN CODES

dig return codes are:

| | |
|---|---|
| 0 | DNS response received, including NXDOMAIN status |
| 1 | Usage error |
| 8 | Couldn't open batch file |
| 9 | No reply from server |
| 10 | Internal error |

## FILES

/etc/resolv.conf

${HOME}/.digrc

## SEE ALSO

delv(1) <#std-iscman-delv>, host(1) <#std-iscman-host>, named(8) <#std-iscman-named>, dnssec-keygen(8) <#std-iscman-dnssec-keygen>, RFC 1035 <https://datatracker.ietf.org/doc/html/rfc1035.html>.

## BUGS

There are probably too many query options.

## Author

Internet Systems Consortium

## Copyright