

Internet Systems Consortium DHCP Distribution
Version 4.3.0a1
17 December 2013

Release Notes

NEW FEATURES

ISC DHCP 4.2.x includes features that were not included in DHCP 4.1.x. These include:

Processing the DHCP to DNS server transactions in an asynchronous fashion. The DHCP server or client can now continue with its processing while awaiting replies from the DNS server.

There are a number of DHCPv6 limitations and features missing in this release, which will be addressed in the future:

- Only Solaris, Linux, FreeBSD, NetBSD, and OpenBSD are supported.
- DHCPv6 includes human-readable text in status code messages, in English. A method to reconfigure or support other languages would be preferable.
- The "host-identifier" option is limited to a simple token.
- The client and server can only operate DHCPv4 or DHCPv6 at a time, not both. To use both protocols simultaneously, two instances of the relevant daemon are required, one with the '-6' command line option.

For information on how to install, configure and run this software, as well as how to find documentation and report bugs, please consult the README file.

ISC DHCP uses standard GNU configure for installation. Please review the output of "./configure --help" to see what options are available.

The system has only been tested on Linux, FreeBSD, and Solaris, and may not work on other platforms. Please report any problems and suggested fixes to <dhcp-users@isc.org>.

Changes since 4.2.0 (new features)

- If a client renews before 'dhcp-cache-threshold' percent of its lease has elapsed (default 25%), the server will reuse the allocated lease (provide a lease within the currently allocated lease-time) rather than extend or renew the lease. This absolves the server of needing to perform an fsync() operation on the lease database before reply, which improves performance. [ISC-Bugs #22228]
Update this patch to support asynchronous DDNS. If the server is attempting to do DDNS on a lease it should be updated and written to disk even if that wouldn't be necessary due to the thresholding [ISC-Bugs #26311]
- The 'no available billing' log line now also logs the name of the last matching billing class tried before failing to provide a billing. [ISC-Bugs #21759]
- A problem with missing get_hw_addr function when --enable-use-sockets was used is now solved on GNU/Linux, BSD and GNU/Hurd systems. Note that use-sockets feature was not tested on those systems. Client and server code no longer use MAX_PATH constant that is not defined on GNU/Hurd systems. [ISC-Bugs #25979]
- Add a perl script in the contrib directory, dhcp-lease-list.pl, which can parse v4 lease files and output the lease information in a more human friendly manner. This was written by Christian Hammers with some updates by vom and ISC. This is contributed code and is not

supported by ISC; however it may be useful to some users.
[ISC-Bugs #20680]

- Add support in v6 for on-commit, on-expire and on-release.
[ISC-Bugs #27912]
- Add support for using classes with v6.
[ISC-Bugs #26510]
- Update the DDNS code to current standards and allow for sharing of DDNS entries between v4 and v6 clients. The new code is used if the ddns-update-style is set to "standard", the older code is still available if ddns-update-style is set to "interim". The oldest DDNS code "ad-hoc" has been removed. Thanks to Thomas Pegeot who submitted a patch for this issue. This patch is based on that work with some modifications.
[ISC-Bugs #21139]
- Add a configuration option to the server to suppress using fsync(). Enabling this option will mean that fsync() is never called. This may provide better performance but there is also a risk that a lease will not be properly written to the disk after it has been issued to a client and before the server stops. Using this option is not recommended.
[ISC-Bugs #34810]
- Add some logging statements to indicate when the server is ready to serve. One statement is emitted after the server has finished reading its files and is about to enter the dispatch loop. This is "Server starting service." The second is emitted when a server determines that both it and its failover peer are in the normal state. This is "failover peer <name>: Both servers normal."
[ISC-Bugs #33208]
- Add support for accessing options from v6 relays. The v6relay statement allows the administrator to choose which relay to use when searching for an option, see the dhcp-options man page for a description. The host-identifier option has also been updated to support the use of relay options see the dhcpd.conf man page for a description.
[ISC-Bugs #19598]
- When doing DDNS if there isn't an appropriate zone statement attempt to find a reasonable nameserver via a DNS resolver. This restores some functionality that was lost in the transition to asynchronous DDNS. Due to the lack of security and increase in fragility of the system when using this feature we strongly recommend the use of appropriate zone statements rather than using this functionality.
[ISC-Bugs #30461]
- Add support for specifying the address from which to send DDNS updates on the DHCP server. There are two new options "ddns-local-address4" and "ddns-local-address6" that each take one instance of their respective address types.
[ISC-Bugs #34779]
- Add ignore-client-uids option in the server. This option causes the server to not record a client's uid in its lease. This violates the specification but may also be useful when a client can dual boot using different client ids but the same mac address. Thank you to Brian De Wolf for the patch.
[ISC-Bugs #32427]
[ISC-Bugs #35066]
- Extend the DHCPINFORM processing to honor the subnet selection option and take host declarations into account.
Thanks to Christof Chen for testing and submitting the patch.

[ISC-Bugs #35015]

Changes since 4.2.5

- Address static analysis warnings.
[ISC-Bugs #33510] [ISC-Bugs #33511]
- Silence benign static analysis warnings.
[ISC-Bugs #33428]
- Add check for 64-bit package for atf.
[ISC-Bugs #32206]
- Use newer auto* tool packages and turn on RFC_3542 support on Mac OS.
[ISC-Bugs #26303]
- Remove a variable when it isn't being used due to #ifdefs to avoid a compiler warning on Solaris using GCC.
[ISC-Bugs #33032]
- Add a check for too much whitespace in a config or lease file.
Thanks to Paolo Pellegrino for finding the issue and a suggestion for the patch.
[ISC-Bugs #33351]
- Fix several problems with using OMAPI to manipulate class and subclass objects.
[ISC-Bugs #27452]
- Added a sleep call after killing the old client to allow time for the sockets to be cleaned. This should allow the -r option to work more consistently.
[ISC-Bugs #18175]
- Missing files for ISC DHCP Developer's Guide are now included in the release tarballs. To generate this documentation, please use make devel command in doc directory. [ISC-Bugs #32767]
- Update client script for use with openwrt.
[ISC-Bugs #29843]
- Fix the socket handling for DHCPv6 clients to allow multiple instances of a client on a single machine to work properly. Previously only one client would receive the packets. Thanks to Jiri Popelka at Red Hat for the bug report and a potential patch.
[ISC-Bugs #34784]
- Added support for gentle shutdown after signal is received.
[ISC-Bugs #32692] [ISC-Bugs 34945]
- Enhance the DHCPv6 server logging to include the addresses that are assigned to the clients.
[ISC-Bugs #26377]

Changes since 4.2.4

- Correct code to calculate timing values in client to compare rebind value to infinity instead of renew value.
Thanks to Chenda Huang from H3C Technologies Co., Limited for reporting this issue.
[ISC-Bugs #29062]
- Fix some issues in the code for parsing and printing options.
[ISC-Bugs #22625] - properly print options that have several fields followed by an array of something for example "fIa"
[ISC-Bugs #27289] - properly parse options in declarations that have several fields followed by an array of something for example "fIa"

[ISC-Bugs #27296] - properly determine if we parsed a 16 or 32 bit value in evaluate_numeric_expression (extract-int).
[ISC-Bugs #27314] - properly parse a zero length option from a lease file. Thanks to Marius Tomaszewski from SUSE for the report and prototype patch for this ticket as well as ticket 27289.

! Previously the server code was relaxed to allow packets with zero length client ids to be processed. Under some situations use of zero length client ids can cause the server to go into an infinite loop. As such ids are not valid according to RFC 2132 section 9.14 the server no longer accepts them. Client ids with a length of 1 are also invalid but the server still accepts them in order to minimize disruption. The restriction will likely be tightened in the future to disallow ids with a length of 1.

Thanks to Markus Hietava of Codenomicon CROSS project for the finding this issue and CERT-FI for vulnerability coordination.

[ISC-Bugs #29851]
CVE: CVE-2012-3571

! When attempting to convert a DUID from a client id option into a hardware address handle unexpected client ids properly. Thanks to Markus Hietava of Codenomicon CROSS project for the finding this issue and CERT-FI for vulnerability coordination.

[ISC-Bugs #29852]
CVE: CVE-2012-3570

! A pair of memory leaks were found and fixed. Thanks to Glen Eustace of Massey University, New Zealand for finding this issue.

[ISC-Bugs #30024]
CVE: CVE-2012-3954

- Existing legacy unit-tests have been migrated to Automated Test Framework (ATF). Several new tests have been developed. To enable unit-tests, please use --with-atf in configure script. A Developer's Guide has been added. To generate it, please use make devel in the doc directory. It is currently in early stages of development, but is expected to grow in the near future. [ISC-Bugs 25901]

! An issue with the use of lease times was found and fixed. Making certain changes to the end time of an IPv6 lease could cause the server to abort. Thanks to Glen Eustace of Massey University, New Zealand for finding this issue.

[ISC-Bugs #30281]
CVE: CVE-2012-3955

- Update the memory leakage debug code to work with v6.
[ISC-Bugs #30297]

- Relax the requirements for deleting an A or AAAA record. Previously the DDNS removal code required both the A or AAAA record and the TXT record to exist. This requirement could cause problems if something interrupted the removal leaving the TXT record alone. This relaxation was codified in RFC 4703.
[ISC-Bugs #30734]

- Modify the failover code to handle incorrect peer names better. Previously the structure holding the name might have been freed inappropriately in some cases and not freed in other cases.
[ISC-Bugs #30320]

- Add a configure option, enable-secs-byteorder, to deal with clients that do the byte ordering on the secs field incorrectly. This field should be in network byte order but some clients get it wrong. When this option is enabled the server will examine the secs field and if it looks wrong (high byte non zero and low byte zero) swap the bytes. The default is disabled. This option

is only useful when doing load balancing within failover.
[ISC-Bugs #26108]

- Fix a set of issues that were discovered via a code inspection tool. Thanks to Jiri Popelka and Tomas Hozza Red Hat for the logs and patches.
[ISC-Bugs #23833]
- Parsing unquoted base64 strings improved. Parser now properly handles strings that contain reserved names. [ISC-Bugs #23048]
- Modify the nak_lease function to make some attempts to find a server-identifier option to use for the NAK.
[ISC-Bugs #25689]
- The client now passes information about the options it requested from the server to the script code via environment variables. These variables are of the form requested_<option_name>=1 with the option name being the same as used in the new_* and old_* variables.
[ISC-Bugs #29068]
- Add support for a simple check that the server id in a request message to a failover peer matches the server id of the server. This support is enabled by editing the file includes/site.h and uncommenting the definition for SERVER_ID_CHECK. The option has several restrictions and issues - please read the comment in the site.h file before enabling it.
[ISC-Bugs #31463]
- Tidy up some compiler issues in the debug code.
[ISC-Bugs #26460]
- Move the dhcpd.conf example file to dhcpd.conf.example to avoid overwriting the dhcpd.conf file when installing a new version of ISC DHCP. The user will now need to manually copy and edit the dhcpd.conf file as desired.
[ISC-Bugs #19337]
- Check the status value when trying to read from a connection to see if it may have been closed. If it appears closed don't try to read from it again. This avoids a potential busy-wait like loop when the peer names are mismatched.
[ISC-Bugs #31231]
- Remove an unused variable to keep compilers happy.
[ISC-Bugs #31983]
- Modify test makefiles to be more similar to standard makefiles and comment out a currently unused test.
[ISC-Bugs #32089]

Changes since 4.2.3

- ! Add a check for a null pointer before calling the regexec function. Without this check we could, under some circumstances, pass a null pointer to the regexec function causing it to segfault. Thanks to a report from BlueCat Networks.
[ISC-Bugs #26704].
CVE: CVE-2011-4539
- ! Modify the DDNS handling code. In a previous patch we added logging code to the DDNS handling. This code included a bug that caused it to attempt to dereference a NULL pointer and eventually segfault. While reviewing the code as we addressed this problem, we determined that some of the updates to the lease structures would not work as planned since the structures being updated were in the process of being freed: these updates were removed. In addition we removed an

incorrect call to the DDNS removal function that could cause a failure during the removal of DDNS information from the DNS server.

Thanks to Jasper Jongmans for reporting this issue.

[ISC-Bugs #27078]

CVE: CVE-2011-4868

- Fixed the code that checks if an address the server is planning to hand out is in a reserved range. This would appear as the server being out of addresses in pools with particular ranges.
[ISC-Bugs #26498]
- In the DDNS code handle error conditions more gracefully and add more logging code. The major change is to handle unexpected cancel events from the DNS client code.
[ISC-Bugs #26287]
- Tidy up the receive calls and eliminate the need for found_pkt.
[ISC-Bugs #25066]
- Add support for Infiniband over sockets to the server and relay code. We've tested this on Solaris and hope to expand support for Infiniband in the future. This patch also corrects some issues we found in the socket code.
[ISC-Bugs #24245]
- Add a compile time check for the presence of the noreturn attribute and use it for log_fatal if it's available. This will help code checking programs to eliminate false positives.
[ISC-Bugs #27539]
- Fixed many compilation problems ("set, but not used" warnings) for gcc 4.6 that may affect Ubuntu 11.10 users. [ISC-Bugs #27588]
- Modify the code that determines if an outstanding DDNS request should be cancelled. This patch results in cancelling the outstanding request less often. It fixes the problem caused by a client doing a release where the TXT and PTR records weren't removed from the DNS.
[ISC-BUGS #27858]
- Use offsetof() instead of sizeof() to get the sizes for dhcpv6_relay_packet and dhcpv6_packet in several more places. Thanks to a report from Bruno Verstuyft and Vincent Demaertelaere of Excentis.
[ISC-Bugs #27941]
- Remove outdated note in the description of the bootp keyword about the option not satisfying the requirement of failover peers for denying dynamic bootp clients.
[ISC-bugs #28574]
- Multiple items to clean up IPv6 address processing.
When processing an IA that we've seen check to see if the addresses are usable (not in use by somebody else) before handing it out.
When reading in leases from the file discard expired addresses.
When picking an address for a client include the IA ID in addition to the client ID to generally pick different addresses for different IAs.
[ISC-Bugs #23138] [ISC-Bugs #27945] [ISC-Bugs #25586]
[ISC-Bugs #27684]
- Remove unnecessary checks in the lease query code and clean up several compiler issues (some dereferences of NULL and treating an int as a boolean).
[ISC-Bugs #26203]
- Fix the NA and PD allocation code to handle the case where a client provides a preference and the server doesn't have any addresses or

prefixes available. Previously the server ignored the request with this patch it replies with a NoAddrAvail or NoPrefixAvail response. By default the code performs according to the errata of August 2010 for RFC 3315 section 17.2.2; to enable the previous style see the section on RFC3315_PRE_ERRATA_2010_08 in includes/site.h. This option may be removed in the future.

Thanks to Jiri Popelka at Red Hat for the patch.
[ISC-Bugs #22676]

- Fix up some issues found by static analysis.
A potential memory leak and NULL dereference in omapi.
The use of a boolean test instead of a bitwise test in dst.
[ISC-Bugs #28941]
- Rotate the lease file when running in v6 mode.
Thanks to Christoph Moench-Tegeder at Astaro for the report and the first version of the patch.
[ISC-Bugs #24887]

Changes since 4.2.2

- Fix the code that checks for an existing DDNS transaction to cancel when removing DDNS information, so that we will continue with the processing if we have a lease even if it doesn't have an outstanding transaction. [ISC-Bugs #24682]
- Add AM_MAINTAINER_MODE to configure.ac to avoid rebuilding configuration files. [ISC-Bugs #24107]
- Add support for passing DDNS information to a DNS server over an IPv6 address. [ISC-Bugs #22647]
- Enhanced patch for 23595 to handle IPv4 fixed addresses more cleanly. [ISC-Bugs #23595]

Changes since 4.2.1

- ! In dhclient check the data for some string options for reasonableness before passing it along to the script that interfaces with the OS.
[ISC-Bugs #23722]
CVE: CVE-2011-0997
- DHCPv6 server now responds properly if client asks for a prefix that is already assigned to a different client. [ISC-Bugs #23948]
- Add the option "--no-pid" to the client, relay and server code, to disable writing a pid file. Add the option "-pf pidfile" to the relay to allow the user to supply the pidfile name at runtime. Add the "with-relay6-pid-file" option to configure to allow the user to supply the pidfile name for the relay in v6 mode at configure time.
[ISC-Bugs #23351] [ISC-Bugs #17541]
- 'dhclient' no longer waits a random interval after first starting up to begin in the INIT state. This conforms to RFC 2131, but elects not to implement a 'SHOULD' direction in section 4.1. The goal of this change is to start up faster. [ISC-Bugs #19660]
- Added 'initial-delay' parameter that specifies maximum amount of time before client goes to the INIT state. The default value is 0. In previous versions of the code client could wait up to 5 seconds. The old behavior may be restored by using 'initial-delay 5;' in the client config file.
[ISC-Bugs #19660]
- ICMP ping-check should now sit closer to precisely the number of seconds configured (or default 1), due to making use of the new microsecond scale timer internally to dhcpd. This corrects a bug where the server

may immediately timeout an ICMP ping-check if it was made late in the current second. [ISC-Bugs #19660]

- The DHCP client will schedule renewal and rebinding events in microseconds if the DHCP server provided a lease-time that would result in sub-1-second timers. This corrects a bug where a 2-second or lower lease-time would cause the DHCP client to enter an infinite loop by scheduling renewal at zero seconds. [ISC-Bugs #19660]
- Client lease records are recorded at most once every 15 seconds. This keeps the client from filling the lease database disk quickly on very small lease times. [ISC-Bugs #19660]
- To defend against RFC 2131 non-compliant DHCP servers which fail to advertise a lease-time (either mangled, or zero in value) the DHCP client now adds the server to the reject list ACL and returns to INIT state to hopefully find an RFC 2131 compliant server (or retry in INIT forever). [ISC-Bugs #19660]
- Parameters configured to evaluate from user defined function calls can now be correctly written to dhcpd.leases (as on 'on events' or dynamic host records inserted via OMAPI). [ISC-Bugs #22266]
- If a 'next-server' parameter is configured in a dynamic host record via OMAPI as a domain name, the syntax written to disk is now correctly parsed upon restart. [ISC-Bugs #22266]
- The DHCP server now responds to DHCPLEASEQUERY messages from agents using IP addresses not covered by a subnet in configuration. Whether or not to respond to such an agent is still governed by the 'allow leasequery;' configuration parameter, in the case of an agent not covered by a configured subnet the root configuration area is examined. Server now also returns vendor-class-id option, if client sent it. [ISC-Bugs #21094]
- Documentation fixes
[ISC-Bugs #17959] add text to AIX section describing how to have it send responses to the all-ones address.
[ISC-Bugs #19615] update the includes in dhcpctl/dhcpctl.3 to be more correct
[ISC-Bugs #20676] update dhcpd.conf.5 to include the RFC numbers for DDNS
- Relay no longer crashes, when DHCP packet is received over interface without any IPv4 address assigned. Also extended logging message about discarding packets with invalid hlen with information about relevant interface name. [ISC-Bugs #22409]
- Relay now properly logs that packet was received over interface without global IPv6 address [ISC-Bugs #24070]
- Linux Packet Filter interface improvement. sockaddr_pkt structure is used, rather than sockaddr. Packet ethertype is now forced to ETH_P_IP. [ISC-Bugs #18975]
- Minor code cleanups - but note port change for #23196
[ISC-Bugs #23470] - Modify when an ignore return macro is defined to handle unused error return warnings for more versions of gcc.
[ISC-Bugs #23196] - Modify the reply handling in the server code to send to a specified port rather than to the source port for the incoming message. Sending to the source port was test code that should have been removed. The previous functionality may be restored by defining REPLY_TO_SOURCE_PORT in the includes/site.h file. We suggest you don't enable this except for testing purposes.
[ISC-Bugs #22695] - Close a file descriptor in an error path.
[ISC-Bugs #19368] - Tidy up variable types in validate_port.
- Code cleanup: remove obsolete PROTO, KandR, INLINE and ANSI_DECL macros [ISC-Bugs #13151]
- Compilation problem with gcc4.5 and omshell.c resolved. [ISC-Bugs #23831]

- Client Script fixes
 - [ISC-Bugs #23045] Typos in client/scripts/openbsd
 - [ISC-Bugs #23565] In the client scripts add a zone id (interface id) if the domain search address is link local.
 - [ISC-Bugs #1277] In some of the client scripts add code to handle the case of the default router information being changed without the address being changed.
- Documentation cleanup
 - [ISC-Bugs #23326] Updated References document, several man page updates
- Server no longer complains about NULL pointer when configured server-identifier expression fails to evaluate. [ISC-Bugs #24547]
- Convert ISC_R_INPROGRESS status to ISC_R_SUCCESS when called from other than the dispatch handler. This fixes an issue where omshell, when run from the same platform as the server, would appear to fail to connect. This is a companion to #21839. [ISC-Bugs #23592]
- Enlarge the buffer size used by the Omshell code and some of the print routines to allow for greater than 60 characters or, when printing as hex strings, 20 characters. [ISC-Bugs #22743]
- In Solaris 11 switch to using sockets instead of DLPI, thanks to a patch from Oracle. [ISC-Bugs #24634].
- Strict checks for content of domain-name DHCPv4 option can now be configured during compilation time. Even though RFC2132 does not allow to store more than one domain in domain-name option, such behavior is now enabled by default, but this may change some time in the future. See ACCEPT_LIST_IN_DOMAIN_NAME define in includes/site.h. [ISC-Bugs #24167]
- DNS Update fix. A misconfigured server could crash during DNS update processing if the configuration included overlapping pools or multiple fixed-address entries for a single address. This issue affected both IPv4 and IPv6. The fix allows a server to detect such conditions, provides the user with extra information and recommended steps to fix the problem. If the user enables the appropriate option in site.h then server will be terminated [ISC-Bugs #23595]
- ! Two packets were found that cause a server to halt. The code has been updated to properly process or reject the packets as appropriate. Thanks to David Zych at University of Illinois for reporting this issue. [ISC-Bugs #24960]
 One CVE number for each class of packet.
 CVE-2011-2748
 CVE-2011-2749

Changes since 4.2.0

- Documentation cleanup covering multiple tickets
 - [ISC-Bugs #20265] [ISC-Bugs #20259] minor cleanup
 - [ISC-Bugs #20263] add text describing some default values
 - [ISC-Bugs #20193] single quotes at the start of a line indicate a control line to nroff, escape them if we actually want a quote.
 - [ISC-Bugs #18916] sync the pointer to web pages amongst the different docs
- 'get-host-names true;' now also works even if 'use-host-decl-names true;' was also configured. The nature of this repair also fixes another error; the host-name supplied by a client is no longer overridden by a reverse lookup of the lease address. Thanks to a patch from Wilco Baan Hofman supplied to us by the Debian package maintenance team. [ISC-Bugs #21691] {Debian Bug#509445}
- The .TH tag for the dhcp-options manpage was typo repaired

thanks to a report from jidanni and the Debian package maintenance team. [ISC-Bugs #21676] {Debian Bug#563613}

- More documentation changes - primarily to put the options in the dhclient and dhcpd man pages into the standard form. Thanks in part to a patch from David Cantrell at Red Hat. [ISC-Bugs #20264] and parts of [ISC-Bugs #17744] dhclient.8 changes
- Add code to clear the pointer to an object in an OMAPI handle when the object is freed due to a dereference. [ISC-Bugs #21306]
- Fixed a bug that leaks host record references onto lease structures, causing the server to apply configuration intended for one host to any other innocent clients that come along later. [ISC-Bugs #22018]
- Minor code fixes
 - [ISC-Bugs #19566] When trying to find the zone for a name for ddns allow the name to be at the apex of the zone.
 - [ISC-Bugs #19617] Restrict length of interface name read from command line in dhcpd - based on a patch from David Cantrell at Red Hat.
 - [ISC-Bugs #20039] Correct some error messages in dhcpd.c
 - [ISC-Bugs #20070] Better range check on values when creating a DHCID.
 - [ISC-Bugs #20198] Avoid writing past the end of the field when adding overly long file or server names to a packet and add a log message if the configuration supplied overly long names for these fields. Thanks to Martin Pala.
 - [ISC-Bugs #21497] Add a little more randomness to rng seed in client thanks to a patch from Jeremiah Jinno.
- Correct error handling in DLPI [ISC-Bugs #20378]
- Remove __sun__ and __hpux__ typedefs in osdep.h as they are now being checked in configure. [ISC-Bugs #20443]
- Modify how the cmsg header is allocated the v6 send and received routines to compile on more compilers. [ISC-Bugs #20524]
- When parsing a domain name free the memory for the name after we are done with it. [ISC-Bugs #20824]
- Add an elapsed time option to the release message and refactor the code to move most of the common code to a single routine. [ISC-Bugs #21171].
- Two identical log messages for commit_leases() have been disambiguated. [ISC-Bugs #18915]
- Parse date strings more properly - the code now handles semi-colons in date strings correctly. Thanks to a patch from Jiri Popelka at Red Hat. [ISC-Bugs #21501, #20598]
- Fixes to lease input and output.
 - [ISC-Bugs #20418] - Some systems don't support the "%s" argument to strftime, paste together the same string using mktime instead.
 - [ISC-Bugs #19596] - When parsing iaid values accept printable characters.
 - [ISC-Bugs #21585] - Always print time values in omshell as hex instead of ascii if the values happen to be printable characters.
- Minor changes for scripts, configure.ac and Makefiles
 - [ISC-Bugs #19147] Use domain-search instead of domain-name in manual and example conf file. Thanks to a patch from David Cantrell at Red Hat.
 - [ISC-Bugs #19761] Restore address when doing a rebind in DHCPv6
 - [ISC-Bugs #19945] Properly close the quote on some arguments.
 - [ISC-Bugs #20952] Add 64 bit types to configure.ac
 - [ISC-Bugs #21308] Add "PATH=" to CLIENT_PATH environment variable

- Update the code to parse dhcpv6 lease files to accept a semi-colon at the end of the max-life and preferred-life clauses. In order to be backwards compatible with older lease files not finding a semi-colon is also accepted. [ISC-Bugs #22303].

- ! Handle a relay forward message with an unspecified address in the link address field. Previously such a message would cause the server to crash. Thanks to a report from John Gibbons. [ISC-Bugs #21992]
CERT: VU#102047 CVE: CVE-2010-3611

- ./configure on longer searches for -lcrypto to explicitly link against. This fixes a bug where 'dhclient' would have shared library dependencies on '/usr/lib'. [ISC-Bugs #21967]

- Handle pipe failures more gracefully. Some OSes pass a SIGPIPE signal to a process and will kill the process if the signal isn't caught. This patch adds code to turn off the SIGPIPE signal via a setsockopt() call. The signal is already being ignored as part of the ISC library. [ISC-Bugs #22269]

- Restore printing of values in omshell to the style pre 21585. For 21585 we changed the print routines to always display time values as a hex list. This had a side effect of printing all data strings as a hex list. We shall investigate other ways of displaying time values more usefully. [ISC-Bugs #22626]

- ! Fix the handling of connection requests on the failover port. Previously a connection request from a source that wasn't listed as a failover peer would cause the server to become non-responsive. Thanks to a report from Brad Bendily, brad@bendily.com. [ISC-Bugs #22679]
CERT: VU#159528 CVE: CVE-2010-3616

- Don't pass the ISC_R_INPROGRESS status to the omapi signal handlers. Passing it through to the handlers caused the omshell program to fail to connect to the server. [ISC-Bugs #21839]

- Fix the paranthesis in the code to process configuration statements beginning with "auth". The previous arrangement caused "auto-partner-down" to be processed incorrectly. [ISC-Bugs #21854]

- Limit the timeout period allowed in the dispatch code to 2³²-1 seconds. Thanks to a report from Jiri Popelka at Red Hat. [ISC-Bugs #22033], [Red Hat Bug #628258]

- When processing the format flags for a given option consume the flag indicating an optional value correctly. A symptom of this bug was an infinite loop when trying to parse the slp-service-scope option. Thanks to a patch from Marius Tomaszewski. [ISC-Bugs #22055]

- Disable the use of kqueue in the ISC library. This avoids a problem between the fork and socket code that caused the dhcpd process to use all available cpu if the program daemonized itself. [ISC-Bugs #21911]

- ! When processing a request in the DHCPv6 server code that specifies an address that is tagged as abandoned (meaning we received a decline request for it previously) don't attempt to move it from the inactive to active pool as doing so can result in the server crashing on an assert failure. Also retag the lease as active and reset its timeout value. [ISC-Bugs #21921]

- Removed the restriction on using IPv6 addresses in IPv4 mode. This allows IPv4 options which contain IPv6 addresses to be specified. For example the 6rd option can be specified and used like this: [ISC-Bugs #23039]

```
option 6rd code 212 = { integer 8, integer 8,  
                          ip6-address, array of ip-address };  
option 6rd 16 10 2001:: 1.2.3.4, 5.6.7.8;
```

- Handle some DDNS corner cases better. Maintain the DDNS transaction information when updating a lease and cancel any existing transactions when removing the ddns information. [ISC-Bugs #23103]
- Some fixes for LDAP [ISC-Bugs #21783] - Include lber library when building ldap [ISC-Bugs #22888] - Enable the ldap code when building common The above fixes are from Jiri Popelka at Red Hat.
- Modify the dlpi code to accept getmsg() returning a positive value. [ISC-Bugs #22824]

Changes since 4.2.0b2

- Add declaration for variable in debug code in alloc.c. [ISC-Bugs #21472]

Changes since 4.2.0b1

- Prohibit including lease time information in a response to a DHCP INFORM. [ISC-Bugs #21092]
- ! Accept a client id of length 0 while hashing. Previously the server would exit if it attempted to hash a zero length client id, providing attackers with a simple denial of service attack. [ISC-Bugs #21253]
CERT: VU#541921 - CVE: CVE-2010-2156
- A memory leak in ddns processing was closed. [ISC-Bugs #21377]
- Modify the exception handling for initial context creation. Previously we would try and clean up before exiting. This could present problems when the cleanup required part of the context that wasn't available. It also didn't do much as we exited afterwards anyway. Now we simply log the error and exit. [ISC-Bugs #21093]
- A bug was fixed that could cause the DHCPv6 server to advertise/assign a previously allocated (active) lease to a client that has changed subnets, despite being on different shared networks. Dynamic prefixes specifically allocated in shared networks also now are not offered if the client has moved. [ISC-Bugs #21152]
- Add some debugging output for use with the DDNS code. [ISC-Bugs #20916]
- Fix the trace code to handle timing events better and to truncate a file before using instead of overwriting it. [ISC-Bugs #20969]
- Modify the determination of the default TTL to use for DDNS updates. The user may still configure the ttl via ddns-ttl. The default for both v4 and v6 is now 1/2 the (preferred) lease time with a limit. The previous defaults (1/2 lease time without a limit for v4 and a default value for v6) may be used by defining USE_OLD_DDNS_TTL in site.h [ISC-Bugs #21126]
- libisc/libdns is now brought up to version 9.7.1rc1. This corrects three reported flaws in ISC DHCP;
 - o DHCP processes (dhcpd, dhclient) fail to start if one of either the IPv4 or IPv6 address families is not present. [ISC-Bugs #21122]
 - o Assertion failure when attempting to cancel a previously running DDNS update. [ISC-Bugs #21133]
 - o Compilation failure of libisc/libdns due to the use of a flexible

array member. [ISC-Bugs #21316]

Changes since 4.2.0a2

- Update the fsync code to work with the changes to the DDNS code. It now uses a timer instead of noticing if there are no more packets to process.
- When constructing the DNS name structure from a text string append the root to relative names. This satisfies a requirement in the DNS library that names be absolute instead of relative and prevents DHCP from crashing. [ISC-Bugs #21054]
- "The LDAP Patch" that has been circulating for some time, written by Brian Masney and S.Kalyanasundaram and maintained for application to the DHCP-4 sources by David Cantrell has been included. Please be advised that these sources were contributed, and do not yet meet the high standards we place on production sources we include by default. As a result, the LDAP features are only included by using a compile-time option which defaults off, and if you enable it you do so under your own recognizance. We will be improving this software over time. [ISC-Bugs #17741]

Changes since 4.2.0a1

- When using 'ignore client-updates;', the FQDN returned to the client is no longer truncated to one octet.
- Cleaned up an unused hardware address variable in nak_lease().
- Manpage entries for the ia-pd and ia-prefix options were updated to reflect support for prefix delegation.
- Cleaned up some compiler warnings
- An optimization described in the failover protocol draft is now included, which permits a DHCP server operating in communications-interrupted state to 'rewind' a lease to the state most recently transmitted to its peer, greatly increasing a server's endurance in communications-interrupted. This is supported using a new 'rewind state' record on the dhcpd.leases entry for each lease.
- Fix the trace code which was broken by the changes to the DDNS code.

Changes since 4.1.0 (new features)

- Failover port configuration can now be left to defaults (port 647) as described in the -12 revision of the Failover draft (and assigned by IANA). Thanks in part to a patch from David Cantrell at Red Hat.
- If configured, dhclient may now transmit to an anycast MAC address, rather than using a broadcast address. Thanks to a patch from David Cantrell at Red Hat.
- Added client support for setting interface MTU and metric, thanks to Roy "UberLord" Marples <roy@marples.name>.
- Added client -D option to specify DUID type to send.
- A new failover configuration parameter has been introduced for those environments where DHCP servers can be reasonably guaranteed to be "down" when the failover TCP socket is severed, "auto-partner-down". This parameter is not generally safe, and by default is disabled, so please carefully review the documentation of this parameter in the dhcpd.conf(5) manpage before determining to use it yourself.
- Added a configuration function, 'gethostname()', which calls the system function of the same name and presents the results as a data expression. This function can be used to incorporate the system level hostname of

the system the DHCP software is operating on in responses or queries (such as including a failover partner's hostname in a dhcp message or binding scope, or having a DHCP client send any system hostname in the host-name or FQDN options by default).

- The dhcp-renewal-time and dhcp-rebinding-time options may now be configured for DHCPv4 operation and used independently of the dhcp-lease-time calculations. Invalid renew and rebinding times (e.g., greater than the determined lease time) are omitted.
- Processing the DHCP to DNS server transactions in an asynchronous fashion. The DHCP server or client can now continue with its processing while awaiting replies from the DNS server.
- The 'hardware [ethernet|etc] ...;' parameter in host records has been extended to attempt to match DHCPv6 clients by the last octets of a DUID-LL or DUID-LLT provided by the client.

Changes since 4.1.0 (bug fixes)

- Remove infinite loop in token_print_indent_concat().
- Validate the argument to the -p option.
- The notorious 'option <unknown> ... larger than buffer' log line, which is seen in some malformed DHCP client packets, was modified. It now logs the universe name, and does not log the length values (which are bogus corruption read from the packet anyway). It also carries a hopefully more useful explanation.
- Suppress spurious warnings from configure about --datarootdir
- A bug was fixed that caused the server not to answer some valid Solicit and Request packets, if the dynamic range covering any requested addresses had been deleted from configuration.
- Update the code to deal with GCC 4.3. This included two sets of changes. The first is to the configuration files to include the use of AC_USE_SYSTEM_EXTENSIONS. The second is to deal with return values that were being ignored.
- The db-time-format option was documented in manpages.
- Using reserved leases no longer results in 'lease with binding state free not on its queue' error messages, thanks to a patch from Frode Nordahl.
- Fix a build error in dhcrelay, using older versions of gcc with dhcpv6 disabled.
- Two uninitialized stack structures are now memset to zero, thanks to a patch from David Cantrell at Red Hat.
- Fixed a cosmetic bug where pretty-printing valid domain-search options would result in an erroneous error log message ('garbage in format string').
- A bug in DLPI packet transmission (Solaris, HP/UX) that caused the server to stop receiving packets is fixed. The same fix also means that the MAC address will no longer appear 'bogus' on DLPI-based systems.
- A bug in select handling was discovered where the results of one select() call were discarded, causing the server to process the next select() call and use more system calls than required. This has been repaired - the sockets will be handled after the first return from select(), resulting in fewer system calls.
- The update-conflict-detection feature would leave an FQDN updated without a DHCID (still currently implemented as a TXT RR). This would cause later

expiration or release events to fail to remove the domain name. The feature now also inserts the client's up to date DHCPID record, so records may safely be removed at expiration or release time. Thanks to a patch submitted by Christof Chen.

- Memory leak in the `load_balance_mine()` function is fixed. This would leak ~20-30 octets per DHCPDISCOVER packet while failover was in use and in normal state.
- Various compilation fixes have been included for the memory related DEBUG #defines in `includes/site.h`.
- Fixed Linux client script 'unary operator expected' errors with DHCPv6.
- Fixed setting hostname in Linux hosts that require hostname argument to be double-quoted. Also allow server-provided hostname to override hostnames 'localhost' and '(none)'.
 - Fixed failover reconnection retry code to continue to retry to reconnect rather than restarting the listener.
- Compilation on Solaris with USE_SOCKETS defined in `includes/site.h` has been repaired. Other USE_ overrides should work better.
- A check for the local flavor of IFNAMSIZ had a broken 'else' condition, that probably still resulted in the correct behaviour (but wouldn't use a larger defined value provided by the host OS).
- Fixed a bug where an OMAPI socket disconnection message would not result in scheduling a failover reconnection, if the link had not negotiated a failover connect yet (e.g.: connection refused, asynch socket connect() timeouts).
- A bug was fixed that caused the 'conflict-done' state to fail to be parsed in failover state records.
 - ! A stack overflow vulnerability was fixed in `dhclient` that could allow remote attackers to execute arbitrary commands as root on the system, or simply terminate the client, by providing an over-long subnet-mask option. CERT VU#410676 - CVE-2009-0692
- Fixed a bug where relay agent options would never be returned when processing a DHCPINFORM.
- Versions 3.0.x syntax with multiple name->code option definitions is now supported. Note that, similarly to 3.0.x, for by-code lookups only the last option definition is used.
- Fixed a bug where a time difference of greater than 60 seconds between a failover pair could cause the primary to crash on contact with the secondary. Thanks to a patch from Steinar Haug.
- Don't look for IPv6 interfaces on Linux when running in DHCPv4 mode. Thanks to patches from Matthew Newton and David Cantrell.
- Secondary servers in a failover pair will now perform ddns removals if they had performed ddns updates on a lease that is expiring, or was released through the primary. As part of the same fix, stale binding scopes will now be removed if a change in identity of a lease's active client is detected, rather than simply if a lease is noticed to have expired (which it may have expired without a failover server noticing in some situations).
- A patch supplied by David Cantrell at RedHat was applied that detects invalid calling parameters given to the `ns_name_ntop()` function. Specifically, it detects if the caller passed a pointer and size pair that causes the pointer to integer-wrap past zero.
 - ! Fixed a fenceposting bug when a client had two host records configured,

one using 'uid' and the other using 'hardware ethernet'. CVE-2009-1892

- Fixed the check in the dhcp_interface_signal_handler routine to verify the existence of the linked signal handler before calling it.
- Both host and subnet6 configuration groups are now included whether a fixed-address6 (DHCPv6) is in use or not. Host scoped configuration takes precedence. This fixes two bugs, one where host scoped configuration would not be included from a non-fixed-address6 host record, and the equal and opposite bug where subnet6 scoped configuration would not be used when over-riding values were not present in a matching fixed-address6 host configuration.
- ./configure now checks to ensure the intX_t and u_intX_t types are defined, correcting a compilation failure when using Sun's compiler.
- Modified the handling of a connection to avoid releasing the omapi io object for the connection while it is still in use. One symptom from this error was a segfault when a failover secondary attempted to connect to the failover primary if their clocks were not synchronized.
- Clean up to allow compilation with gcc 2.95.4 on FreeBSD. Remove an extra semi-colon from common/dns.c and moved setting a variable to NULL in server/dhcpv6.c to allow the compiler to decide that the variable was always properly set.

Changes since 4.1.0b1

- A missing "else" in dhcrelay.c could have caused an interface not to be recognized.

Changes since 4.1.0a2

- A cosmetic bug in DHCPDECLINE processing was fixed which caused all successful DHCPDECLINEs to be logged as "not found" rather than "abandoned".
- Added configuration file examples for DHCPv6.
- Some failover debugging #defines have been better defined and some high frequency messages moved to a deeper debugging symbol.
- The CLTT parameter in failover is now only updated by client activity, and not by failover binding updates (taking on the peer's CLTT).
- Failover BNDUPD messages are now discarded if they conflict with an update that has been transmitted, but not acknowledged.
- A bug cleaning up unknown-xxx temporary option definitions was fixed.
- Delayed-ack is now a compile-time option, compiled out by default. This feature is simply too experimental for right now, and causes some problems to some failover installations. We will revisit this in future releases.
- The !inet_pton() call in res_mkupdrec was adjusted to '<= 0' as inet_pton returns either 1, 0, or -1.
- A dhclient-script for MacOS X has been included, which enables 'dhclient -6' support.
- DDNS removal routines were updated so that the DHCID is not removed until the client has been deprived of all A and AAAA records (not only the last one of either of those). This resolves a bug where dual stack clients would not be able to regain their names after either expiration event.

Changes since 4.1.0a1

- Corrected list of failover state values in dhcpd man page.
- Fixed a bug that caused some request types to be logged incorrectly.
- Clients that sent a parameter request list containing the routers option before the subnet mask option were receiving only the latter. Fixed.
- The server wasn't always sending the FQDN option when it should.
- A partner-down failover server no longer emits 'peer holds all free leases' if it is able to newly-allocate one of the peer's leases.
- Fixed a coredump when adding a class via OMAPI.
- Check whether files are zero length before trying to parse them.
- Ari Edelkind's PARANOIA patch has been included and may be compiled in via two ./configure parameters, --enable-paranoia and --enable-early-chroot.
- ./configure was extended to cover many optional build features, such as failover, server tracing, debugging, and the execute() command.
- There is now a default 1/4 of a second scheduled delay between delayed fsync()'s, it can be configured by the max-ack-delay configuration parameter.
- A bug was fixed where the length of a hostname was miscalculated, so that hosts were given odd-looking domain names ("foo.bar.ba.example.com").
- Shared network selection should be done from the innermost relay valid link-address field, rather than the outermost.
- Prefix pools are attached to shared network scopes.
- Merged IA_XX related structures.
- Add DHCPv6 files in configure.
- A memory leak when using omapi has been fixed.
- DHCPv6 vendor-class options (VSI0) are now only sent when they appear on the DHCPv6 ORO. This resolves a bug where VSI0 options were placed in IA_NA encapsulated options fields.
- Integrated client with stateless, temporary address and prefix delegation support.
- A double-dereference in dhclient transmission of DHCPDECLINEs was repaired.
- Fix handling of format code 'Z'.
- Support "-1" argument in DHCPv6.
- Merge DHCPv6-only "dhcrelay6" into general-purpose "dhcrelay" (use "-6" option to select DHCPv6 mode).
- Fix handling of -A and -a flags in dhcrelay; it was failing to expand packet size as needed to add relay agent options.
- A bug in subnet6 parsing where options contained in subnet6 clauses would not be applied to clients addressed within that network was repaired.
- When configuring a "subnet {}" or "subnet6 {}" without an explicit shared-network enclosing it, the DHCP software would synthesize a shared-network to contain the subnet. However, all configuration

parameters within the subnet more intuitively belong "to any client on that interface", or rather the synthesized shared-network. So, when a shared-network is synthesized, it is used to contain the configuration present inside the subnet {} clause. This means that the configuration will be valid for all clients on that network, not just those addressed out of the stated subnet. If you intended the opposite, the workaround is to explicitly configure an empty shared-network.

- A bug was fixed where Information-Request processing was not sourcing configured option values.
- A warning was added since the DHCPv6 processing software does not yet support class statements.
- Compilation warnings on GCC 4.3 relating to bootp source address selection were repaired.
- The v6 BSD socket method was updated to use a single UDP BSD socket no matter how many interfaces are involved, differentiating the interfaces the packets were received on by the interface index supplied by the OS.
- The relay agent no longer listens to the All DHCP Servers Multicast address.
- A bug was fixed in data_string_sprintf() where va_start was only called once for two invocations of vsprintf() variants.
- ERO (RFC 4994) server support.
- Basic and partial DHCPv6 leasequery support.
- Reliable DHCPv6 release (previous behavior, send release and exit, is still available with dhclient -6 -1 -r).

Changes since 4.0.0 (new features)

- Added DHCPv6 rapid commit support.
- Added explicit parser support for zero-length DHCP options, such as rapid-commit, via format code 'Z'.
- It's now possible to update the "ends" field of a lease with OMAPI. This is useful if you want not only to release a lease, but also make it available for reuse right away. Hat tip to Christof Chen.
- Fixed definition of the iaaddr hash functions to use the correct functions when referencing and dereferencing memory.
- Some definitions not in phase with the IANA registry were updated.
- Allocated interface IDs are better controlled ('u' bit set to zero, reserved IDs avoided).
- Unicast options are taken into account only for RENEWs.
- NoAddrsAvail answers to SOLICITs are always ADVERTISEs even when a SOLICIT carries a rapid-commit option.
- Return in place of raise an impossible condition when one tries to release an empty active lease.
- Timer granularity is now 1/100s in the DHCPv6 client.
- The dhclient-script was updated to create a host route for the default gateway if the supplied subnet mask for an IPv4 address was a /32. This allows the client to work in 'captive' network environments, where the

operator does not want clients to crosstalk directly.

- MINUS tokens should be parseable again.
- Multiple (up to "delayed-ack x;" maximum) DHCPv4 packets are now queued and released in bursts after single fsync() events when the upper limit is reached or if the receiving sockets go dry. The practical upshot is that fsync-coupled server performance is now multiplicatively increased. The default delayed ack limit is 28. Thanks entirely to a patch from Christof Chen.

Changes since 4.0.0 (bug fixes)

- DHCP now builds on AIX.
- Exit with warning when DHCPv6-specific statements are used in the config file but -6 is not specified.
- Fixed "--version" flag in dhcrelay
- The 'min-secs' configuration parameter's log message has been updated to be more helpful.
- The warning logged when an address range doesn't fit in the subnets they were declared has been updated to be more helpful and identify the typo in configuration that created the spanning addresses.
- A bug in failover pool rebalancing that caused POOLREQ message ping-pongs was repaired.
- A flaw in failover pool rebalancing that could cause POOLREQ messages to be sent outside of the min-balance/max-balance scheduled intervals has been repaired.
- A cosmetic bug during potential-conflict recovery that caused the peer's 'conflict-done' state message to be logged as 'unknown-state' has been repaired. It is now logged correctly.
- A bug was fixed where the 'giaddr' may be used to find the client's subnet rather than its own 'ciaddr'.
- A log message was introduced to clarify the situation where a failover 'address' parameter (the server's local address) did not resolve to an IPv4 address.
- The minimum site code value was set to 224 in 3.1.0 to track RFC3942. This broke a lot of legacy site local configurations. The new code in place will track site local space minimum option codes and logs a warning to encourage updates and exploration of site local code migration problems. Option codes less than 128 in site local spaces remain inaccessible.
- A possible relay agent option bug was repaired where random server initialization state may have been used to signal the relay agent information options sub-option code for the 'END' of the option space.
- Fixes to allow code to compile and run on Solaris 9.
- Fixes to allow code to compile on Mac OS X Leopard (10.5).
- When server is configured with options that it overrides, a warning is issued when the configuration file is read, rather than at the time the option is overridden. This was important, because the warning was given every time the option was overridden, which could create a lot of unnecessary logging.
- Fixed a compilation problems on platforms that define a value for FDDI, which conflicts with a dhcp configuration syntax token by the same name.

- When a failover server suspects it has encountered a peer running a version 3.0.x failover server, a warning that the failover wire protocol is incompatible is printed.
- The failover server no longer issues a floating point error if it encounters a previously undefined option code.
- Fix startup error messages to report a missing "subnet6 declaration", rather than a missing "subnet declaration", when running as a DHCPv6 server.
- DHCPv6 client timestamp in DUID was based on the year 1970 rather than the year 2000.
- Warn when attempting to use a hardware parameter in DHCPv6.
- DHCPv6 released resources are now marked as released by the client.
- 'Soft' bindings have no more side-effects.

Changes since 4.0.0b3

- The reverse dns name for PTR updates on IPv6 addresses has been fixed to use ip6.arpa. rather than default to in-addr.arpa and require user configuration.
- dhc6_lease_destroy() and dhc6_ia_destroy() now set lease and IA pointers to NULL after freeing, to prevent subsequent accesses to freed memory.
- The DHCPv6 server would not send the preference option unless the client requested it, via the ORO. This has been fixed, so the DHCPv6 server will always send the preference value if it is configured.
- When addresses were passed as hints to the server in an IA, they were incorrectly handled, sometimes being treated as an error. Now the server will treat these as hints and ignore them if it cannot supply a requested address.
- If the client had multiple addresses, and one expired (was not renewed by the server), the client would continue to attempt to renew the same old address over and over. Now, the client will omit any expired addresses from future Confirm, Renew, or Rebind messages.
- dhclient -6 will now select renew/rebind timers based upon the longest address expiration time rather than the shortest expiration time, in order to avoid cascading renewals in the event a server elects not to extend one of multiple IAADDR leases.
- The server now limits clients that request multiple addresses to one address per IA by default, which can be adjusted through the "limit-addr-per-ia" configuration option.
- The DHCPv6 client now issues fresh transaction IDs on Renew and Rebind message exchanges, rather than using the most recent ID.
- The DHCPv6 server now replies to Information-Request messages.
- A bug was fixed in the dhclient-script for BSDs to correctly carry error codes through some conditions.
- The parsing of some options in the dhclient lease file, in particular the success DHCPv6 status-code, was fixed.
- A bug was fixed that caused the DHCPv6 ORO option to be corrupted with seemingly random values.
- A reference overleak in DHCPv6 shared network processing was repaired.
- ./configure now autodetects local database locations rather than trying

to put `dhcpd.leases` and `dhclient.leases` in `/usr/local/var/db`, which no one ever has.

- Regression fix for bug where server advertised a IPv6 address in response to a SOLICIT but would not return the address in response to a REQUEST.
- A bug was fixed where the DHCPv6 server puts the NoAddrsAvail status code in the IA_NA was fixed. The status code now appears in the root level.

Changes since 4.0.0b2

- Clarified error message when lease limit exceeded
- Relative time may now be used as a qualifier for 'allow' and 'deny' access control lists. These directives may be used to assist in re-addressing address pools without having to constantly reconfigure the server. Please see 'man dhcpd.conf' for more information on allow/deny 'after time' syntax. Thanks to a patch from Christof Chen.
- The server will now include multiple IA_NA's and multiple IAADDRs within them, if advertised by the client. It still only seeks to allocate one new address.

Changes since 4.0.0b1

- Use different paths for PID and lease files when running in DHCPv4 or DHCPv6 mode, so that servers for both protocols can be run simultaneously on a single interface.
- Fixed a buffer overflow error which could have allowed a denial of service under unusual server configurations
- Eliminated a spurious error message from the client
- A number of bugs with the internal handling of lease state on the server have been fixed. Some of these could cause server crashes.
- The `peer_wants_leases()` changes pulled up from 3.1.0 were corrected, 'never used' leases will no longer consistently shift between servers on every pool rebalance run.
- `sendmsg()/recvmsg()` control buffers are now declared in such a way to ensure they are correctly aligned on all (esp. 64-bit) architectures.
- The client leasing subsystem was streamlined and corrected to account more closely for changes in client link attachment selection.

Changes since 4.0.0a3

- The DHCP server no longer requires a "ddns-update-style" statement, and now defaults to "none", which means DNS updates are disabled.
- Log messages when failover peer names mismatch have been improved to point out the problem.
- Bug where server advertised a IPv6 address in response to a SOLICIT but would not return the address in response to a REQUEST. Thanks to Dennis Kou for finding the bug.
- Fixed an error causing the server to lock up on lease expiration, reported independently by Jothilingam Vasu and Dennis Kou.
- Fixed a `./configure` bug where compile tests were failing due to "-Werror" (unused variable) rather than the actual test failure. Lead to inconsistent and unworkable auto-configurations.

- Compilation with DLPI and `-Werror` has been repaired.
- Error in decoding IA_NA option if multiple interfaces are present fixed by Marcus Goller.
- DHCPv6 server Confirm message processing has been enhanced - it no longer replies only to clients with host {} records, it now replies as directed in RFC3315 section 18.2.2 - that is, to all clients regardless of the existence of bindings.
- A core dump during expired lease cleanup has been repaired.
- DDNS updates state information are now stored in 'binding scopes' that follow the leases through their lifecycles. This enables DDNS teardowns on leases that are assigned and expired inbetween a server restart (the state is recovered from `dhcpd.leases`). Arbitrary user-specified binding scopes ('set var = "value";') are not yet supported.
- Additional compilation problems on HP/UX have been repaired.

Changes since 4.0.0a2

- Fix for startup where there are no IPv4 addresses on an interface. Thanks to Marcus Goller for reporting the bug.
- Fixed file descriptor leak on listen failure. Thanks to Tom Clark.
- Bug in server configuration parser caused server to get stuck on startup for certain bad pool declarations. Thanks to Guillaume Knispel for the bug report and fix.
- Code cleaned to remove warnings reported by "`gcc -Wall`".
- DHCPv6 is now the default. You can disable DHCPv6 support using the "`--disable-dhcpv6`" flag when you run the configure script.
- An internal database inconsistency bug was repaired where the server would segfault if a client attempted to renew a lease that had been loaded from persistent storage.
- 'request' and 'also request' syntaxes have been added to accommodate the DHCPv6 client configuration. 'send dhcp6.oro' is no longer necessary.
- Bug fixed where configuration file parsing did not work with zero-length options; this made it impossible to set the `rapid-commit` option.
- Bogus messages about host records with IPv4 fixed-addresses being of non-128-bits in length were removed.

Changes since 4.0.0a1

- Bug in octal parsing fixed. Thanks to Bernd Fuhrmann for the report and fix.
- Autoconf now supplies proper flags for Solaris DHCPv6 builds.
- Fix for parsing error on some IPv6 addresses.
- Invalid CIDR representation for IPv6 subnets or ranges now checked for when loading configuration.
- Compilation on HP/UX has been repaired. The changes should generally apply to any architecture that supplies `SIOCLIFCONF` but does not use 'struct lifconf' structures to pass values.
- Two new operators, `~=` and `~`, have been integrated to implement

boolean matches by regular expression (such as may be used in class matching statements). Thanks to a patch by Alexandr S. Agranovsky, which underwent slight modification.

- Fix for icmp packets on 64-bit systems (bug introduced in 4.0).
- A bug was fixed in interface discovery wherein an error identifying a server-configured interface with no IPv4 addresses would SEGV.
- Fixed a bug in which write_lease() might report a failure incorrectly
- Added support for DHCPv6 Release messages
- Added -x option to dhclient, which triggers dhclient processes to exit gracefully without releasing leases first
- All binaries (client, server, relay) now change directories to / before going into daemon mode, so as not to hold \$CWD open
- Fixed a bug parsing DHCPv6 client-id's in host-identifier statements
- Fixed a bug with the 'ddns-updates' boolean server configuration parameter, which caused the server to fail.

Changes since 4.0.0-20070413

- Old (expired) leases are now cleaned.
- IPv6 subnets now have support for arbitrary allocation ranges via a new 'range6' configuration directive.
- An obviated option code hash lookup to find D60_CLIENTID was removed.
- Corrected some situations where variables might be used without being initialized.
- Silenced several other compiler warnings.
- Include the more standard sys/uio.h rather than rely upon other header files to include it (fixes a BSD 4.2 compile failure).
- Duplicate dhclient-script updates for DHCPv6 to all provided scripts.
- DHCPv4 I/O methods that failed to sense hardware address were corrected.
- DHCPv4 is now the default (as documented) rather than DHCPv6. The default was set to DHCPv6 to facilitate ease early development, and forgotten.
- Corrected a segmentation violation in DHCPv4 socket processing.
- dhclient will now fork() into the background once it binds to an IPv6 address, or immediately if the -n flag is supplied.
- -q is now the default behaviour on dhclient, with -d or -v enabling non-quiet (stderr logging) mode.
- Fix documentation of the domain-search atom (quoted, with commas).
- Document DHCPv6 options presently in the default table.
- Replaced ./configure shellscripting with GNU Autoconf.

Changes since 3.1.0 (NEW FEATURES)

- DHCPv6 Client and Server protocol support. Use '-6' to run the daemons as v6-only. Use '-4' to run the daemons as v4-only (default). There is no support currently for both.

- Server support for multiple IA_NA options, containing at most one IAADDR option.
- Client support for one IA_NA option, containing any number of IAADDR options.
- Server support for the DHCPv6 Information-request message.
- Inappropriate unicast DHCPv6 messages sent to the server are now discarded, and this has rearchitected the IO system slightly.
- The DHCPv6 server DUID defaults to type 1, is persistently stored in the leases database, and can be over-ridden (either completely, or by specifying type 1 or type 2).
- The server only uses Rapid-Commit if it has been configured with the Rapid-Commit option and the client requests it.
- DDNS support. We now update AAAA records in the same place we would update A records, if we have an IPv6 address. We also generate IP6.ARPA style names for PTR records if we're dealing with an IPv6 address. Both A and AAAA updates are done using the same 'fqdn.' virtual option space (although the DHCPv4 FQDN and DHCPv6 FQDN options are formatted differently, they both use the same code here).
- The Linux dhclient-script attempts to set and remove assigned addresses, and to configure /etc/resolv.conf from nameserver and domain name configurations. It can be extended to configure other parameters.
- Initial DHCPv6 lease support.
- The IO system now tracks all local IP addresses, so that the DHCP applications (particularly the dhcrelay) can discern between what frames were transmitted to it, and what frames are being carried through it which it should not intercept.

Changes since 3.1.0 (Maintenance)

- A bug was repaired where MAC Address Affinity for virgin leases always mapped to the primary. Virgin leases now have an interleaved preference between primary and secondary.
- A bug was repaired where MAC Address Affinity for clients with no client identifier was sometimes mishashed to the peer. Load balancing during runtime and pool rebalancing were opposing.
- An assertion in lease counting relating to reserved leases was repaired.
- The subnet-mask option inclusion now conforms with RFC2132 section 3.3; it will only appear prior to the routers option if it is present on the Parameter-Request-List. The subnet-mask option will also only be included by default (if it is not on the PRL) in response to DISCOVER or REQUEST messages.
- The FQDN option is only supplied if the client supplied an FQDN option or if the FQDN option was explicitly requested on the PRL.
- Dynamic BOOTP leases are now load balanced in failover.

Changes since 3.1.0rc1

- The parse warning that 'deny dyanmic bootp;' must be configured for failover protected subnets was removed.

Changes since 3.1.0b2

- Failover rebalance events no longer play ping pong with round errors (moving leases between free and back to backup where there are an

odd number of leases).

- The 'pool' log line has been split into two messages, one before the rebalance run, and one after.
- Any queued BNDACKs are transmitted before transmitting new BNDUPDs. This enforces the correct sequence of events for the remote server processing these messages.

Changes since 3.1.0b1

- Fixed a bug that caused OMAPI clients to freeze when opening lease objects.
- A new server config option "fqdn-reply" specifies whether the server should send out option 81 (FQDN). Defaults to "on". If set to "off", the FQDN option is not sent, even if the client requested it. This is needed because some clients misbehave otherwise. Thanks to Christof Chen at Allianz.
- Allow trace output files (-tf option) to be overwritten, rather than crashing dhcpd if the file already exists
- A bug was fixed that caused dhcpd to segfault if a pool was declared outside the scope of a subnet in dhcpd.conf.
- Some uninitialized values were repaired in dhcpleasequery.c that caused the server to abort.
- A new server config option, 'do-reverse-updates', has been added which causes the server to abstain from performing updates on PTR records. Thanks to a patch from Christof Chen at Allianz.
- A bug was repaired in subencapsulation support, where spaces separated by empty spaces would not get included.
- A bug in dhclient was repaired which caused it to send parameter request lists of 55 bytes in length no matter how long the declared PRL was.
- 'dhcp.c(3953): non-null pointer' has been repaired. This fixes a flaw wherein the DHCPv4 server may ignore a configured server-identifier.
- A flaw in failover startup sequences was repaired that sometimes left the primary DHCP server's pool rebalance schedules unscheduled.
- Corrected a flaw that broke encapsulated spaces included due to presence on the parameter request list.

Changes since 3.1.0a3

- Some spelling fixes.

Changes since 3.1.0a2

- A bug was fixed where attempting to permit leasequeries results in a fatal internal error, "Unable to find server option 49".
- A bug was fixed in dhclient rendering the textual output form of the domain-search option syntax.

Changes since 3.1.0a1

- A bug in the FQDN universe that added FQDN codes to the NWIP universe's hash table was repaired.
- The servers now try harder to transmit pending binding updates when entering normal state.

- UPDREQ/UPDREQALL handling was optimized - it no longer dequeues and requeues all pending updates. This should reduce the number of spurious 'xid mismatch' log messages.
- An option definition referencing leak was fixed, which resulted in early termination of dhclient upon the renewal event.
- Some default hash table sizes were tweaked, some upwards, some downwards. 3.1.0a1's tables resulted in a reduction in default server memory use. The new selected values provide more of a zero sum (increasing the size of tables likely to be populated, decreasing the size of tables unlikely).
- Lease structures appear in three separate hashes: by IP address, by UID, and by hardware address. One type of table was used for all three, and improvements to IP address hashing were applied to all three (so UID and hardware addresses were treated like 4-byte integers). There are now two types of tables, and the uid/hw hashes use functions more appropriate to their needs.
- The max-lease-misbalance percentage no longer causes scheduled rebalance runs to be skipped: it still governs the schedule, but every scheduled run will attempt balance.
- A segfault bug in recursive encapsulation support has been corrected.

Changes since 3.0 (New Features)

- A workaround for certain STSN servers that send a mangled domain-name option was introduced for dhclient. The client will now accept corrupted server responses, if they contain a valid DHCP_MESSAGE_TYPE (OFFER, ACK, or NAK). The server will continue to not accept corrupt client packets.
- Support for 'reserved' (pseudo-static) and BOOTP leases via failover was introduced.
- Support for adding, removing, and managing class and subclass statements via OMAPI.
- The failover implementation was updated to comply with revision 12 of the protocol draft.
- 'make install' now creates the initial zero-length dhcpd.leases file if one does not already exist on the system.
- RFC3942 compliance, site-local option spaces start at 224 now, not 128.
- The Load Balance Algorithm was misimplemented. The current implementation matches RFC 3074.
- lcase() and ucase() configuration expressions have been added which adjust their arguments from upper to lower and lower to upper cases respectively. Thanks to a patch from Albert Herranz.
- The dhclient 'reject ...;' statement, which rejects leases given by named server-identifiers, now permits address ranges to be specified in CIDR notation. Thanks to a patch from David Boyce.
- The subnet-mask option is now supplied by default, but at lowest priority. This helps a small minority of clients that provide parameter request lists, but do not list the subnet-mask option because they were designed to interoperate with a server that behaves in this manner.
- The FQDN option is similarly supplied even if it does not appear on the parameter request list, but not to the exclusion of options that do appear at the parameter request list. Up until now it had ultimate priority over the client's parameter request list.
- Varying option space code and length bit widths (8/16/32) are now

supported. This is a milestone in achieving RFC 3925 "VIVSO" and DHCPv6 support.

- A new common (server or client) option, 'db-time-format local;', has been added which prints the local time in /var/db/dhcpd.leases rather than UTC. Thanks to a patch from Ken Lalonde.
- Some patches to improve DHCP Server startup speed from Andrew Matheson have been incorporated.
- Failover pairs now implement 'MAC Affinity' on leases moving from the active to free states. Leases that belonged to the failover secondary are moved to BACKUP state rather than FREE upon exiting EXPIRED state. If lease rebalancing must move leases, it tries first to move leases that belong to the peer in need.
- The server no longer sends POOLREQ messages unless the pool is severely misbalanced in the peer's favor (see 'man dhcpd.conf' for more details).
- Pool rebalance events no longer happen upon successfully allocating a lease. Instead, they happen on a schedule. See 'man dhcpd.conf' for the min-balance and max-balance statements for more information.
- The DHCP Relay Agent Information Option / Link Selection Sub-Option is now supported. (See RFC3527 for details).
- A new DDNS related server option, update-conflict-detection, has been added. If this option is enabled, dhcpd will perform normal DHCID conflict resolution (the default). If this option is disabled, it will instead trust the assigned name implicitly (removing any other bindings on that name). This option has not been made available in dhclient.
- In those cases where the DHCP software manufactures an IP header (to transmit via bpf, lpf, etc), the IP TTL the software selects has been increased from 16 to 128. This is intended to match Microsoft Windows DHCP Client behaviour, to increase compatibility.
- 'ignore client-updates;' now has behaviour that is different from 'deny client-updates;'. The client's request is not truly ignored, rather it is encouraged. Should this value be configured, the server updates DNS as though client-updates were set to 'deny'. That is, it enters into DNS whatever it is configured to do already, provided it is configured to. Then it sends a response to the client that lets the client believe it is performing client updates (which it will), probably for a different name. In essence, this lets the client do as it will, ignoring this aspect of their request.
- Support for compressed 'domain name list' style DHCP option contents, and in particular the domain search option (#119) was added.
- The DHCP LEASEQUERY protocol as defined in RFC4388 is now implemented. LEASEQUERY lets you query the DHCP server for information about a lease, using either an IP address, MAC address, or client identifier. Thanks to a patch from Justin Haddad.
- DHCPD is now RFC2131 section 4.1 compliant (broadcast to all-ones ip and ethernet mac address) on the SCO platform specifically without any strange ifconfig hacks. Many thanks go to the Kroger Co. for donating the hardware and funding the development.
- A new common configuration executable statement, execute(), has been added. This permits dhcpd or dhclient to execute a named external program with command line arguments specified from other configuration language. Thanks to a patch written by Mattias Ronnblom, gotten to us via Robin Breathe.
- A new dhcp server option 'adaptive-lease-time-threshold' has been added which causes the server to substantially reduce lease-times if there are

few (configured percentage) remaining leases. Thanks to a patch submitted from Christof Chen.

- Encapsulated option spaces within encapsulated option spaces is now formally supported.

Changes since 3.0.6rc1

- `supersede_lease()` now requeues leases in their respective hardware address hash bucket. This mirrors client identifier behaviour.

Changes since 3.0.5

- Assorted fixes for broken network devices: Packet length is now determined from the IP header length field to finally calculate the UDP payload length, because some NIC drivers return more data than they actually received.
- UDP packets are now stored in aligned data structures.
- A logic error in `omapi` interface code was repaired that might result in incorrectly indicating 'up' state when any flags were set, rather than specifically the `INTERFACE_REQUESTED` flag. Thanks to a patch from Jochen Voss which got to us via Andrew Pollock at Debian.
- A reference leak on binding scopes set by `ddns` updates was repaired.
- A memory leak in the `minires_nsendsigned()` function call was repaired. Effectively, this leaked ~176 bytes per DDNS update.
- In the case where an "L2" DHCP Relay Agent (one that does not set `giaddr`) was directly attached to the same broadcast domain as the DHCP server, the RFC3046 relay agent information option was not being returned to the relay in the server's replies. This was fixed; the `dhcp` server no longer requires the `giaddr` to reply with relay agent information. Note that this also improves compatibility with L2 devices that "intercept" DHCP packets and expect relay agent information even in unicast (renewal) replies. Thanks to a patch from Pekka Silvonon.
- A bug was fixed where the BOOTP header 'sname' field had a value, the copy written to persistent storage was actually the contents of the 'file' field.
- A bug was fixed where the `nwip` virtual option space was referencing the `fqdn` option's virtual option space's option cache.
- Timestamp parsing errors that indicated missing "minutes" fields rather than the actually missing "seconds" fields have been repaired thanks to a patch from Kevin Steves.
- A grammar error in the `dhclient.8` manpage was repaired thanks to a patch from Chris Wagner.
- Several spelling typos were repaired, and some cross-references to other relevant documents were included in the manpages, thanks to a patch by Andrew Pollock which got to us via Tomas Pospisek.
- Some bugs were fixed in the 'emergency relay agent options hologram' which is used to retain relay agent option contents from when the client was in `INIT` or `REBIND` states. This should solve problems where relay agent options were not echoed from the server, even when `giaddr` was set.
- `dhclient` now closes its descriptor to `dhclient.leases` prior to executing `dhclient-script`. Thanks to a patch from Tomas Pospisek.
- The server's "by client-id" and "by hardware address" hash table lists are now sorted according to the preference to re-allocate that lease to

returning clients. This should eliminate pool starvation problems arising when "INIT" clients were given new leases rather than presently active ones.

Changes since 3.0.5rc1

- A bug was repaired in fixes to the dhclient, which sought to run the dhclient-script with the 'EXPIRE' state should it receive a NAK in response to a REQUEST. The client now iterates the PREINIT state after the EXPIRE state, so that interfaces that might be configured 'down' can be brought back 'up' and initialized.
- DHCPINFORM handling for clients that properly set ciaddr and come to the server via a relay agent has been repaired.

Changes since 3.0.4

- A warning that host statements declared within subnet or shared-network scopes are actually global has been added.
- The default minimum lease time (if min-lease-time was not specified) was raised from 0 to 300. 0 is not thought to be sensible, and is known to be damaging.
- Added additional fatal error sanity checks surrounding lease binding state count calculations (free/active counts used for failover pool balancing).
- Some time value size fixes in 3.0.4 brought on from FreeBSD /usr/ports were misapplied to server values rather than client values. The server no longer advertises 8-byte lease-time options when on 64-bit platforms.
- A bug where leases not in ACTIVE state would get billed to billed classes (classes with lease limitations) was fixed. Non-active leases OFFERed to clients are no longer billed (but billing is checked before offering).
- The dhcpd.conf.5 manpage was updated in regard to the ddns-domainname configuration option - the default configuration and results should be more clear now.
- If the dhclient were to receive a DHCPNAK while it was in the RENEW state (and consequently, had an active, 'bound' address and related configuration options), it would fail to 'tear down' this information before proceeding into INIT state. dhclient now iterates the dhclient-script with the 'EXPIRE' action to cause these teardowns prior to entering INIT state. Thanks to a patch from Chris Zimmerman.
- The omapi.1 manpage had some formatting errors repaired thanks to a patch from Yoshihiko Sarumaru.
- A few lines of code that were failover-specific were moved within #if defined() clauses so that compilation without failover could be made possible.
- The log message emitted when the 'leased-address' value was not available in dhcpd.conf "executable statements" has been updated to be more helpful. Manpage information for this value has also been updated.
- Abandoned or dissociated (err condition) leases now remove any related dynamic dns bindings. Thanks to a patch from Patrick Schoo.
- Attempting to write a new lease file to replace a corrupt (due to encountering non-retryable errors during writing) lease file should no longer result in an infinite recursion.
- Host declaration hardware addresses and client identifiers may only be configured once. dhcpd will now fail to load config files that specify multiple identifiers (previous versions would silently over-ride the

value with the later configured value).

- Several option codes that have been allocated since our last release have been named and documented.
- Option names of the form "unknown-123" have been removed from the in-memory hash tables. In order to support options of these names that may appear in dhclient.leases or similar in previous versions, the parser will now find the new option code definition, or mock up a generic option code definition. This should result in a smooth transition from one name to the other, as the new name is used to write new output.

Changes since 3.0.4rc1

- The dhcp-options.5 manpage was updated to correct indentation errors thanks to a patch from Jean Delvare.

Changes since 3.0.4b3

- Some manual pages were clarified pursuant to discussion on the dhcp-server mailing list.

Changes since 3.0.4b2

- Null-termination sensing for certain clients that unfortunately require it in DHCPINFORM processing was repaired.
- The host-name option and a few others were moved from "X" format to "t" format to be compatible with new NULL handling functions.
- DHCPINFORM processing is a little more careful about return addressing its responses, or if responding via a relay. The INFORM related messages also log the 'effective client ip address' rather than the client's supplied ciaddr (since some clients produce null ciaddrs).
- The server was inappropriately sending leases to the RESET state in the event that multiple active leases were found to match a singly-identified client. This was changed to RELEASED (by accepting a different, ACTIVE binding, the client is implicitly releasing its lease). This repairs a bug wherein secondary servers in failover pairs detecting this condition move leases to RESET, and primaries refuse to accept that state transition (properly).
- The memset-after-dmalloc() changes made in 3.0.4b1 have been backed out.

Changes since 3.0.4b1

- Command line parsing in omshell was repaired - it no longer closes STDIN after reading one line.
- The resolver library no longer closes the /etc/resolv.conf file descriptor it opened twice.
- Changes to trailing NULL removal in 't' option-atoms has been rethought, it now includes 'd' (domain name) types, and tries hard not to rewind an option beyond the start of the text field it is un-terminating.

Changes since 3.0.3

- A DDNS update handling function was misusing the DNS error codes, rather than the internal generic result enumeration. The result is a confusing syslog line, logging the wrong condition.
- The DHCP Server was not checking pool balance in the case where it brought a non-ACTIVE lease out of storage for a client that was returning to use a lease it once had long ago, and had since expired.

- Failover peers no longer bother to look for free leases to allocate when they already found the client's ACTIVE lease. DISCOVERs are load balanced whether freely-allocated or not, unless the server doubts the peer has leases to allocate.
- Fixed a bug in dhcrelay agent addition code that suppressed trailing PAD options - it was suppressing only one trailing PAD option, rather than the entire block of them.
- ! Fixed some unlikely overlapping-region memcpy() bugs in dhcrelay agent option addition and stripping code. Added a few sanity checks. Although highly improbable, due to requiring the reception of a DHCP datagram well in excess of all known to be used physical MTU limitations, it is possible this may have been used in a stack overflow security vulnerability. Thanks to a patch from infamous42md.
- ! Added some sanity checks to OMAPI connection/authentication code. Although highly improbable, due to having to deliver in excess of 2^32 bytes of data via the OMAPI channel, not to mention requiring dhcpd to be able to malloc() a memory region 2^32 bytes in size, it was possible this might have resulted in a heap overflow security vulnerability. Thanks to a patch from infamous42md.
- dmalloc() memset()'s the non-debug (data) portion of the allocated memory to zero. Code that memset()'s the result returned by dmalloc() to zero is redundant. These redundancies were removed.
- Some type declaration corrections to u_int16_t were made in common/tr.c (Token Ring support) thanks to a patch from Jason Vas Dias at Red Hat.
- A failover bug that was allowing leases that EXPIRED or were RELEASED where tsfp and tstp are identical timestamps to languish in these transitional states has been repaired. As a side effect, lease databases should be kept more consistent overall, not just for these transitional states.
- If the lease db is deleted out from under the daemon, and it moves to rewrite the db, it will go ahead with the operation and move the new db into place once it detects the old db does not exist.
- dhclient now ignores IRDA, SIT, and IEEE1394 network interfaces, as it is either nonsensical or (in the case of IEEE1394) is not known to support these interfaces. Thanks to Marius Gedminas and Andrew Pollock of Debian.
- Some previously undocumented reasons for dhclient-script invoking has been documented in the dhclient-script.8 manpage.
- Failover potential expiry calculations (TSTP) have been corrected. Results should be substantially more consistent, and proper given the constraints.
- Adjusted lease state validation checks in potential-conflict, to account for possible clock skew similarly to normal state, and several previously illegal transitions were made legal (ex: active->released).
- An impossible sanity check was removed from omapi/buffer.c, thanks to a patch from 'infamous42md'.
- An OMAPI host/network byte order problem in lease time values has been repaired.
- Several minor bugs, largely relating to treating 8-byte time values as 4-byte entities, have been repaired after careful review of the FreeBSD ports collection's patch set. Thanks to the nameless entities who have contributed to the FreeBSD ports.
- When writing a trace file, the file is now created with permissions 0600, to help administrators avoid accidentally publicising sensitive config data.

- The calculation of the maximum size of DHCP packets no longer includes Ethernet framing overhead. The result is that the 'Maximum Message Size' option advertised by clients, or the default value 576, is no longer reduced by 14 bytes, and instead directly reflects the IP level MTU (and the default, minimum allowed IP MTU of 576).
- The special status of RELEASED/EXPIRED/RESET leases when a server is operating in partner-down was fixed. It no longer requires a lease be twice the MCLT beyond STOS to 'reallocate', and the expiry event to turn these into FREE leases without peer acknowledgement (after STOS+MCLT) has been repaired.
- Compilation on older Solaris systems (lacking /usr/include/sys/int_types.h) has been repaired.
- "append"ing a string onto the end of a "t" type option (such as the domain-name field) that had been improperly NULL-terminated by the DHCP server will no longer result in a truncated string containing only the option from the server, and not the expected appended value. Thanks to a patch from Jason Vas Dias at Red Hat.
- File handlers on configuration state (config files and lease dbs) should be treated consistently, regardless of whether TRACING is defined or not.
- The Linux build environment has had some minor improvements - better sensing of 64-bit pointer sizes (only used for establishing an icmp_id), and corrections to #if operators regarding LINUX_MAJOR should it ever move to 3.[01].x.
- The server now tries harder to survive the condition where it is unable to open a new lease file to rewrite the lease state database.

Changes since 3.0.3b3

- dhclient.conf documentation for interface {} was updated to reflect recent discussion on the dhcp-hackers mailing list.
- In response to reports that the software does not compile on GCC 4.0.0, -Werror was removed from Makefile.conf for all platforms that used it. We will address the true problem in a future release; this is a temporary workaround.

Changes since 3.0.3b2

- An error in code changes introduced in 3.0.3b2 was corrected, which caused static BOOTP clients to receive random addresses.

Changes since 3.0.3b1

- A bug was fixed in BOOTPREQUEST handling code wherein stale references to host records would be left behind on leases that were not allocated to the client currently booting (eg in the case where the host was denied booting).
- The dhcpd.conf.5 manpage was updated to be more clear in regards to multiple host declarations (thanks to Vincent McIntyre). 'Interim' style dynamic updates were also retouched.

Changes since 3.0.2

- A bug was fixed where a server might load balance a DHCP REQUEST to its peer after already choosing not to load balance the preceding DISCOVER. The peer cannot allocate the originating server's lease.
- In the case where a secondary server lost its stable storage while the primary was still in communications-interrupted, and came back online, the lease databases would not be fully transferred to the secondary. This was due to the secondary errantly sending an extra UPDREQ message

when the primary made its state transition to PARTNER-DOWN known.

- The package will now compile cleanly in gcc 3.3 and 3.4. As a side effect, lease structures will be 9 bytes smaller on all platforms. Thanks to Jason Vas Dias at Red Hat.
- Interface discovery code in DISCOVER_UNCONFIGURED mode is now properly restricted to only detecting broadcast interfaces. Thanks to a patch from Jason Vas Dias at Red Hat.
- decode_udp_ip_header was changed so that the IP address was copied out to a variable, rather than referenced by a pointer. This enforces 4-byte alignment of the 32-bit IP address value. Thanks to a patch from Dr. Peter Poeml.
- An incorrect log message was corrected thanks to a patch from Dr. Peter Poeml.
- A bug in DDNS was repaired, where if the server's first DDNS action was a DDNS removal rather than a DDNS update, the resolver library's retransmit timer and retry timer was set to the default, implying a 15 second timeout interval. Which is a little excessive in a synchronous, single-threaded system. In all cases, ISC DHCP should now hold fast to a 1-second timeout, trying only once.
- The siaddr field was being improperly set to the server-identifier when responding to DHCP messages. RFC2131 clarified the siaddr field as meaning the 'next server in the bootstrap process', eg a tftp server. The siaddr field is now left zeroed unless next-server is configured.
- mockup_lease() could have returned in an error condition (or in the condition where no fixed-address was found matching the shared network) with stale references to a host record. This is probably not a memory leak since host records generally never die anyway.
- A bug was repaired where failover servers would let stale client identifiers persist on leases that were reallocated to new clients not sending an id.
- Binding scopes ("set var = value;") are now removed from leases allocated by failover peers if the lease had expired. This should help reduce the number of stale binding scopes on leases.
- A small memory leak was closed involving client identifiers larger than 7 bytes, and failover.
- Configuring a subnet in dhcpd.conf with a subnet mask of 32 bits might cause an internal function to overflow heap. Thanks to Jason Vas Dias at Red Hat.
- Some inconsistencies in treating numbers that the lexer parsed as 'NUMBER' or 'NUMBER_OR_NAME' was repaired. Hexadecimal parsing is affected, and should work better.
- In several cases, parse warnings were being issued before the lexical token had been advanced to the token whose value was causing an error... causing parse warnings to claim the problem is on the wrong token.
- Host declarations matching on client identifier for dynamic leases will no longer match fixed-address host declarations (this is now identical to behaviour for host records matching on hardware address).

Changes since 3.0.2rc3

- A previously undocumented configuration directive, 'local-address', was documented in the dhcpd.conf manpage.

Changes since 3.0.2rc2

- Two variables introduced in 3.0.2b1 were used without being initialized in the case where neither the FILE nor SNAME fields were available for overloading. This was repaired.
- A heretofore believed to be impossible corner case of the option overloading implementation turned out to be possible ("Unable to sort overloaded options after 10 tries."). The implementation was reworked to consider the case of an option so large it would require more than three chunks to fit.
- Many other instances of variables being used without being initialized were repaired.
- An uninitialized variable in omapi_io_destroy() led to the discovery that this function may result in orphaned pointers (and hence, a memory leak).

Changes since 3.0.2rc1

- allocate_lease() was rewritten to repair a bug in which the server would try to allocate an ABANDONED lease when FREE leases were available.

Changes since 3.0.2b1

- Some dhcp-eval.5 manpage formatting was repaired.

Changes since 3.0.1

- A bug was fixed in the server's 'option overloading' implementation, where options loaded into the 'file' and 'sname' packet fields were not aligned precisely as rfc2131 dictates.
- The FreeBSD client script was changed to support the case where a domain name was not provided by the server.
- A memory leak in 'omshell' per each command line parsed was repaired, thanks to a patch from Jarkko Torppa.
- Log functions writing to stderr were adjusted to use the STDERR_FILENO system definition rather than '2'. This is a no-op for 90% of platforms.
- One call to trace_write_packet_iov() counted the number of io vectors incorrectly, causing inconsistent tracefiles. This was fixed.
- Some expression parse failure memory leaks were closed.
- A host byte order problem in tracefiles was repaired.
- Pools configured in DHCPD for failover possessing permission lists that previously were assumed to not include dynamic bootp clients are now a little more pessimistic. The result is, dhcpd will nag you about just about most pools that possess a 'allow' statement with no 'deny' that would definitely match a dynamic bootp client.
- The 'ddns-update-style' configuration warning bit now insists that the configuration be globally scoped.
- Two memory leaks in dhclient were closed thanks to a patch from Felix Farkas.
- Some minor but excellently pedantic documentation errors were fixed thanks to a patch from Thomas Klausner.
- Bugs in operator precedence in executable statements have been repaired once again. More legal syntaxes should be parsed legally.
- Failing to initialize a tracefile for any reason if a tracefile was specified is now a fatal error. Thanks to a patch from Albert Herranz.

- Corrected a bug in which the number of leases transferred as calculated by the failover primary and sent to peers in POOLRESP responses may be incorrect. This value is not believed to be used by other failover implementations, excepting perhaps as logged information.
- Corrected a bug in which 'dhcp_failover_send_poolresp()' was in fact sending POOLREQ messages instead of POOLRESP messages. This message was essentially ignored since failover secondaries effectively do not respond to POOLREQ messages.
- Type definitions for various bitwidths of integers in the sunos5-5 build of ISC DHCP have been fixed. It should compile and run more easily when built in 64-bit for this platform.
- "allow known-clients;" is now a legal syntax, to avoid confusion.
- If one dhcp server chooses to 'load balance' a request to its failover peer, it first checks to see if it believes said peer has a free lease to allocate before ignoring the DISCOVER.
- log() was logging a work buffer, rather than the value returned by executing the statements configured by the user. In some cases, the work buffer and the intended results were the same. In some other cases, they were not. This was fixed thanks to a patch from Gunnar Fjone and directconnect.no.
- Compiler warnings for some string type conversions was fixed, thanks to Andreas Gustafsson.
- The netbsd build environments were simplified to one, in which -Wconversion is not used, thanks to Andreas Gustafsson.
- How randomness in the backoff-cutoff dhclient configuration variable is implemented was better documented in the manpage, and the behaviour of dhclient in REQUEST timeout handling was changed to match that of DISCOVER timeout handling.
- Omapi was hardened against clients that pass in null values, thanks to a patch from Mark Jason Dominus.
- A bug was fixed in dhclient that kept it from doing client-side ddns updates. Thanks to a patch from Andreas Gustafsson, which underwent some modification after review by Jason Vas Dias.
- Failover implementations disconnected due to the network between them (rather than one of the two shutting down) will now try to re-establish the failover connection every 5 seconds, rather than to simply try once and give up until one of them is restarted. Thanks to a patch from Ulf Ekberg from Infoblox, and field testing by Greger V. Teigre which led to an enhancement to it.
- A problem that kept DHCP Failover secondaries from tearing down ddns records was repaired. Thanks to a patch from Ulf Ekberg from Infoblox.
- 64bit pointer sizes are detected properly on FreeBSD now.
- A bug was repaired where the DHCP server would leave stale references to host records on leases it once thought about offering to certain clients. The result would be to apply host and 'known' scopes to the wrong clients (possibly denying booting). NOTE: The 'mis-host' patch that was being circulated as a workaround is not the way this bug was fixed. If you were a victim of this bug in 3.0.1, you are cautioned to proceed carefully and see if it fixes your problem.
- A bug was repaired in the server's DHCPINFORM handling, where it tried to divine the client's address from the source packet and

would get it wrong. Thanks to Anshuman Singh Rawat.

- A log message was introduced to help illuminate the case where the server was unable to find a lease to assign to any BOOTP client. Thanks to Daniel Baker.
- A minor dhcpd.conf.5 manpage error was fixed.

Changes since 3.0.1rc14

- The global variable 'cur_time' was centralized and is now uniformly of a type #defined in system-dependent headers. It had previously been defined in one of many places as a 32-bit value, and this causes mayhem on 64-bit big endian systems. It probably wasn't too healthy on little endian systems either.
- A printf format string error introduced in rc14 was repaired.
- AIX system-dependent header file was altered to only define NO_SNPRINTF if the condition used to #ifdef in vsnprintf in AIX' header files is false.
- The Alpha/OSF system-dependent header file was altered to define NO_SNPRINTF on OS revisions older than 4.0G.
- omapip/test.c had string.h added to its includes.

Changes since 3.0.1rc13

- ! CAN-2004-0460 - CERT VU#317350: Five stack overflow exploits were closed in logging messages with excessively long hostnames provided by the clients. It is highly probable that these could have been used by attackers to gain arbitrary root access on systems using ISC DHCP 3.0.1 release candidates 12 or 13. Special thanks to Gregory Duchemin for both finding and solving the problem.
- ! CAN-2004-0461 - CERT VU#654390: Once the above was closed, an opening in log_*(*) functions was evidenced, on some specific platforms where vsnprintf() was not believed to be available and calls were wrapped to sprintf() instead. Again, credit goes to Gregory Duchemin for finding the problem. Calls to snprintf() are now linked to a distribution-local snprintf implementation, only in those cases where the architecture is not known to provide one (see includes/cf/[arch].h). If you experience linking problems with snprintf/vsnprintf or 'isc_print_' functions, this is where to look. This vulnerability did not exist in any previously published version of ISC DHCP.
- Compilation on hpux 11.11 was repaired.
- 'The cross-compile bug fix' was backed out.

Changes since 3.0.1rc12

- Fixed a bug in omapi lease lookup function, to form the hardware address for the hash lookup correctly, thanks to a patch from Richard Hirst.
- Fixed a bug where dhcrelay was sending relayed responses back to the broadcast address, but with the source's unicast mac address. Should now conform to rfc2131 section 4.1.
- Cross-compile bug fix; use \$(AR) instead of ar. Thanks to Morten Brorup.
- Fixed a crash bug in dhclient where dhcpd servers that do not provide renewal times results in an FPE. As a side effect, dhclient can now properly handle 0xFFFFFFFF (-1) expiry times supplied by servers. Thanks to a patch from Burt Silverman.

- The 'ping timeout' debugs from rc12 were removed to -DDEBUG only, and reformatted to correct a compilation error on Solaris platforms.
- A patch was applied which fixes a case where leases read from the leases database do not properly over-ride previously read leases.
- dhcpctl.3 manpage was tweaked.

Changes since 3.0.1rc11

- A patch from Steve Campbell was applied with minor modifications to permit reverse dns PTR record updates with values containing spaces.
- A patch from Florian Lohoff was applied with some modifications to dhcrelay. It now discards packets whose hop count exceeds 10 by default, and a command-line option (-c) can be used to set this threshold.
- A failover bug relating to identifying peers by name length instead of by name was fixed.
- Declaring failover configs within shared-network statements should no longer result in error.
- The -nw command line option to dhclient now works.
- Thanks to a patch from Michael Richardson:
 - Some problems with long option processing have been fixed.
 - Some fixes to minires so that updates of KEY records will work.
- contrib/ms2isc was updated by Shu-Min Chang of the Intel Corporation. see contrib/ms2isc/readme.txt for revision notes.
- Dhclient no longer uses shell commands to kill another instance of itself, it sends the signal directly. Thanks to a patch from Martin Blapp.
- The FreeBSD dhclient-script was changed so that a failure to write to /etc/resolv.conf does not prematurely end the script. This keeps dhclient from looping infinitely when this is the case. Thanks to a patch from Martin Blapp.
- A patch from Bill Stephens was applied which resolves a problem with lease expiry times in failover configurations.
- A memory leak in configuration parsing was closed thanks to a patch from Steve G.
- The function which discovers interfaces will now skip non-broadcast or point-to-point interfaces, thanks to a patch from David Brownlee.
- Options not yet known by the dhcpd or dhclient have had their names changed such that they do not contain # symbols, in case they should ever appear in a lease file. An option that might have been named "#144" is now "unknown-144".
- Another patch from Bill Stephens which allows the ping-check timeout to be configured as 'ping-timeout'. Defaults to 1.

Changes since 3.0.1rc10

- Potential buffer overflows in minires repaired.
- A change to the linux client script to use /bin/bash, since /bin/sh may not be bash.
- Some missing va_end cleanups thanks to a patch from Thomas Klausner.
- A correction of boolean parsing syntax validation - some illegal syntaxes

that worked before are now detected and produce errs, some legal syntaxes that errored before will now work properly.

- Some search-and-replace errors that caused some options to change their names was repaired.
- Shu-min Chang of the Intel corporation has contributed a perl script and module that converts the MS NT4 DHCP configuration to a ISC DHCP3 configuration file.
- Applied the remainder of the dhcpctl memory leak patch provided by Bill Squier at ReefEdge, Inc. (groo@reefedge.com).
- Missing non-optional failover peer configurations will now result in a soft error rather than a null dereference.

Changes since 3.0.1rc9

- A format string was corrected to fix compiler warnings.
- A number of spelling corrections were made in the man pages.
- The dhclient.conf.5 man page was changed to refer to do-forward-updates rather than a configuration option that doesn't exist.
- A FreeBSD-specific bug in the interface removal handling was fixed.
- A Linux-specific Token Ring detection problem was fixed.
- Hashes removed from as-yet-unknown agent options, having those options appear in reality before we know about them will no longer produce self-corrupting lease databases.
- dhclient will use the proper port numbers now when using the -g option.
- A order-of-operations bug with 2 match clauses in 1 class statement is fixed thanks to a patch from Andrew Matheson.
- Compilation problems on Solaris were fixed.
- Compilation problems when built with DEBUG or DEBUG_PACKET were repaired.
- A fix to the dhcp ack process which makes certain group options will be included in the first DHCP OFFER message was made thanks to a patch from Ling Gou.
- A few memory leaks were repaired thanks to patches from Bill Squier at ReefEdge, Inc. (groo@reefedge.com).
- A fix for shared-networks that sometimes give clients options for the wrong subnets (in particular, 'option routers') was applied, thanks to Ted Lemon for the patch.
- Omshell's handling of dotted octets as values was changed such that dots one after the other produce zero values in the integer string.

Changes since 3.0.1rc8

- Fix a format string vulnerability in the server that could lead to a remote root compromise (discovered by NGSEC Research Team, www.ngsec.com).
- Add additional support for NetBSD/sparc64.
- Fix a bug in the command-line parsing of the client. Also, resolve a memory leak.
- Add better support for shells other than bash in the Linux client script.

- Various build fixes for modern versions of FreeBSD and Linux.
- Fix a bad bounds check when printing binding state names.
- Clarify documentation about fixed-address and multiple addresses.
- Fix a typo in the authoritative error message.
- Make a log entry when we can't write a billing class.
- Use conversion targets that are the right size on all architectures.
- Increment the hop count when relaying.
- Log a message when lease state is changed through OMAPI.
- Don't rerun the shared_network when evaluating the pool.
- Fix a reversed test in the parser.
- Change the type of rbuf_max.
- Make FTS_LAST a manifest constant to quiet warnings.

Changes since 3.0.1rc7

- Fix two compiler warnings that are generated when compiling on Solaris with gcc. These stop the build, even though they weren't actually errors, because we prefer that our builds generate no warnings.

Changes since 3.0.1rc6

- Don't allow a lease that's in the EXPIRED, RELEASED or RESET state to be renewed.
- Implement lease stealing for cases where the primary has fewer leases than the secondary, as called for by the standard.
- Add a fudge factor to the lease expiry acceptance code, (suggested by Kevin Miller of CMU).
- Fix a bug in permit_list_match that made it much too willing to say that two permit lists matched.
- Unless DEBUG_DNS_UPDATES is defined, print more user-friendly (and also more compact) messages about DNS updates.
- Fix a bug in generating wire-format domain names for the FQDN option.
- Fix a bug where the FQDN option would not be returned if the client requested it, contrary to the standard.
- On Darwin, use the FreeBSD DHCP client script.
- On NetBSD/sparc, don't check for casting warnings.
- Add a flag in the DHCP client to disable updating the client's A record when sending an FQDN option indicating that the client is going to update its A record.
- In the client, don't attempt a DNS update until one second after configuring the new IP address, and if the update times out, keep trying until a response, positive or negative, is received from the DNS server.
- Fix an uninitialized memory bug in the DHCP client.

- Apply some FreeBSD-specific bug fixes suggested by Murray Stokely.
- Fix a bug in ns_parserr(), where it was returning the wrong sort of result code in some cases (suggested by Ben Harris of the NetBSD project).
- Fix a bug in is_identifier(), where it was checking against EOF instead of the END_OF_FILE token (also suggested by Ben Harris).
- Fix a bug where if an option universe contained no options, the DHCP server could dump core (Walter Steiner).
- Fix a bug in the handling of encapsulated options.
- Fix a bug that prevented NWIP suboptions from being processed.
- Delete the FTS_BOOTP and FTS_RESERVED states and implement them as modifier flags to the FTS_ACTIVE state, as called for in the failover protocol standard.
- Fix bugs in the pool merging code that resulted in references and dereferences of null pointers. This bug had no impact unless the POINTER_DEBUG flag was defined.
- In the server, added a do-forward-updates flag that can be used to disable forward updates in all cases, so that sites that want the clients to take sole responsibility for updating their A record can do so.
- Make it possible to disable optimization of PTR record updates.

Changes since 3.0.1rc5

- Include some new documentation and changes provided by Karl Auer.
- Add a workaround for some Lexmark printers that send a double-NUL-terminated host-name option, which would break DNS updates.
- Fix an off-by-one error in the MAC-address checking code for DHCPRELEASE that was added in 3.0.1rc5.
- Fix a bug where client-specific information was not being discarded from the lease when it expired or was released, resulting in problems if the lease was reallocated to a different client.
- If more than one allocation pool is specified that has the same set of constraints as another allocation pool on the same shared network, merge the two pools.
- Don't print an error in fallback_discard, since this just causes confusion and does not appear to be helping to encourage anyone to fix this bug.

Changes since 3.0.1rc4

- Fix a bug that would cause the DHCP server to spin if asked to parse a certain kind of incorrect statement.
- Fix a related bug that would prevent an error from being reported in the same case.
- Additional documentation.
- Make sure that the hardware address matches the lease when processing a DHCPRELEASE message.

Changes since 3.0.1rc3

- A minor bug fix in the arguments to a logging function call.
- Documentation update for dhcpd.conf.

Changes since 3.0.1rc2

- Allow the primary to send a POOLREQ message. This isn't what the current failover draft says to do, so we may have to back it out if I can't get the authors to relent, but the scheme for balancing that's specified in the current draft seems needlessly hairy, so I'm floating a trial balloon. The rc1 code did not implement the method described in the draft either.

Changes since 3.0.1rc1

- Treat NXDOMAIN and NXRRSET as success when we are trying to delete a domain or RRSET. This allows the DHCP server to forget about a name it added to the DNS once it's been removed, even if the DHCP server wasn't the one that removed it.
- Install defaults for failover maximum outstanding updates and maximum silent time. This prevents problems that might occur if these values were not configured.
- Don't do DDNS deletes if ddns-update-style is none.
- Return relay agent information options in DHCPNAK. This prevents DHCPNAK messages from being dropped when the relay agent information option contains routing information.
- Fix a problem where coming up in recover wouldn't result in an update request being sent.
- Add some more chatty messages when we start a recovery update and when it's done.
- Fix a possible problem where some state might have been left around after the peer lost contact and regained contact about how many updates were pending.
- Don't nix a lease update because of a lease conflict. This test has never (as far as I know) prevented a mistake, and it appears to cause problems with failover.
- Add support in rc history code for keeping a selective history, rather than a history of all references and dereferences. This code is only used when extensive additional debugging is enabled.

Changes since 3.0

- Make allocators for hash tables. As a side effect, this fixes a memory smash in the subclass allocation code.
- Fix a small bug in omshell where if you try to close an object when no object is open, it dumps core.
- Fix an obscure coredump that could occur on shutdown.
- Fix a bug in the recording of host declaration rubouts in the lease file.
- Fix two potential spins in the host deletion code.
- Fix a core dump that would happen if an application tried to update a host object attribute with a null value.

Changes since 3.0 Release Candidate 12

- Fix a memory leak in the evaluation code.
- Fix an obscure core dump.

- Print a couple of new warnings when parsing the configuration file when crucial information is left out.
- Log "no free leases" as an error.
- Documentation updates.

Changes since 3.0 Release Candidate 11

- Always return a subnet selection option if one is sent.
- Fix a warning that was being printed because an automatic data structure wasn't zeroed.
- Fix some failover state transitions that were being handled incorrectly.
- When `supersede_lease` is called on a lease whose end time has already expired, but for which a state transition has not yet been done, do a state transition. This fixes the case where if the secondary allocated a lease to a client and the lease "expired" while the secondary was in partner-down, no expiry event would actually happen, so the lease would remain active until the primary was restarted.

Changes since 3.0 Release Candidate 10

- Fix a bug that was preventing released leases from changing state in failover-enabled pools.
- Fix a core dump in the client identifier finder code (for host declarations).
- Finish fixing a bug where bogus data would sometimes get logged to the `dhclient.leases` file because it was opened as descriptor 2.
- Fix the Linux `dhclient-script` according to suggestions made by several people on the `dhcp-client` mailing list.
- Log successful DNS updates at `LOG_INFO`, not `LOG_ERROR`.
- Print an error message and refuse to run if a failover peer is defined but not referenced by any pools.
- Correct a confusing error message in failover.

Changes since 3.0 Release Candidate 9

- Fix a bug in lease allocation for Dynamic BOOTP clients.

Changes since 3.0 Release Candidate 8 Patchlevel 2

- Fix a bug that prevented `update-static-leases` from working.
- Document failover-state OMAPI object.
- Fix a compilation error on SunOS 4.

Changes since 3.0 Release Candidate 8 Patchlevel 1

- Fix a parsing bug that broke dns updates (both interim and ad-hoc). This was introduced in `rc8pl1` as an unintended result of the memory leakage fixes that were in `pl1`.
- Fix a long-standing bug where the server would record that an update had been done for a client with no name, even though no update had been done, and then when the client's lease expired the deletion of

that nonexistent record would time out because the name was the null string.

- Clean up the omshell, dhcpctl and omapi man pages a bit.

Changes since 3.0 Release Candidate 8

- Fix a bug that could cause the DHCP server to spin if one-lease-per-client was enabled.
- Fix a bug that was causing core dumps on BSD/os in the presence of malformed packets.
- In partner-down state, don't restrict lease lengths to MCLT.
- On the failover secondary, record the MCLT received from the primary so that if we come up without a connection to the primary we don't wind up giving out zero-length leases.
- Fix some compilation problems on BSD/os.
- Fix a bunch of memory leaks.
- Fix a couple of bugs in the option printer.
- Fix an obscure error reporting bug in the dns update code, and also make the message clearer when a key algorithm isn't supported.
- Fix a bug in the tracing code that prevented trace runs that used tcp connections from being played back.
- Add some additional debugging capability for catching memory leaks on exit.
- Make the client release the lease correctly on shutdown.
- Add some configurability to the build system.
- Install omshell manual page in man1, not man8.
- Craig Gwydir sent in a patch that fixes a long-standing bug in the DHCP client that could cause core dumps, but that for some reason hadn't been noticed until now.

Changes since 3.0 Release Candidate 7

- Fix a bug in failover where we weren't sending updates after a transition from communications-interrupted to normal.
- Handle expired/released/reset -> free transition according to the protocol specification (this works - the other way not only wasn't conformant, but also didn't work).
- Add a control object in both client and server that allows either daemon to be shut down cleanly.
- When writing a lease, if we run out of disk space, shut down the output file and insist on writing a new one before proceeding.
- In the server, if the OMAPI listener port is occupied, keep trying to get it, rather than simply giving up and exiting.
- Support fetching variables from leases and also updating and adding variables to leases via OMAPI.
- If two failover peers have wildly different clocks, refuse to start doing failover.

- Fix a bug in the DNS update code that could cause core dumps when running on alpha processors.
- Fixed a bug in ddns updates for static lease entries, thanks to a patch from Andrey M Linkevitch.
- Add support for Darwin/MacOS X
- Install omshell (including new documentation).
- Support DNS updates in the client (this is a very obscure feature that most DHCP client users probably will not be able to use).
- Somewhat cleaner status logging in the client.
- Make OMAPI key naming syntax compatible with the way keys are actually named (key names are domain names).
- Fix a bug in the lease file writer.
- Install DHCP ISC headers in a different place than BIND 9 ISC headers, to avoid causing trouble in BIND 9 builds.
- Don't send updates for attributes on an object when the attributes haven't changed. Support deleting attributes on remote objects.
- Fix a number of bugs in omshell, and add the unset and refresh statements.
- Handle disconnects in OMAPI a little bit more intelligently (so that the caller gets ECONNRESET instead of EINVAL).
- Fix a bunch of bugs in the handling of clients that have existing leases when they try to renew their leases while failover is operating.

Changes since 3.0 Release Candidate 6

- Fix a core dump that could happen when processing a DHCPREQUEST from a client that had a host declaration that contained both a fixed-address declaration and a dhcp-client-identifier option declaration, if the client identifier was longer than nine bytes.
- Fix a memory leak that could happen in certain obscure cases when using omapi to manipulate leases.
- Fix some bugs and omissions in omshell.

Changes since 3.0 Release Candidate 5

- Fix a bug in omapi_object_dereference that prevented objects in chains from having their reference counts decreased on dereference.
- Fix a bug in omapi_object_dereference that would prevent object chains from being freed upon removal of the last reference external to the chain.
- Fix a number of other memory leaks in the OMAPI protocol subsystem.
- Add code in the OMAPI protocol handler to trace memory leakage.
- Clean up the memory allocation/reference history printer.
- Support input of dotted quads and colon-separated hex lists as attribute values in omshell.
- Fix a typo in the Linux interface discovery code.

- Conditionalize a piece of trace code that wasn't conditional.

Changes since 3.0 Release Candidate 4

- Fix a bug that would prevent leases from being abandoned properly on DHCPDECLINE.
- Fix failover peer OMAPI support.
- In failover, correctly handle expiration of leases. Previously, leases would never be reclaimed because they couldn't make the transition from EXPIRED to FREE.
- Fix some broken failover state transitions.
- Documentation fixes.
- Take out an unnecessary check in DHCP relay agent information option stashing code that was preventing REBINDING clients from rebinding.
- Prevent failover peers from allocating leases in DHCPREQUEST processing if the lease belongs to the other server.
- Record server version in lease file introductory comment.
- Correctly report connection errors in OMAPI and failover.
- Make authentication signature algorithm name comparisons in OMAPI case-insensitive.
- Fix compile problem on SunOS 4.x
- If a signature algorithm is not terminated with '.', terminate it so that comparisons between fully-qualified names will work consistently.
- Different SIOCGIFCONF probe code, may "fix" problem on some Linux systems with the probe not working correctly.
- Don't allow user to type omapi key on command line of omshell.

Changes since 3.0 Release Candidate 3

- Do lease billing on startup in a way that I *think* will finally do the billing correctly - the previous method could overbill as a result of duplicate leases.
- Document OMAPI server objects.

Changes since 3.0 Release Candidate 2 Patchlevel 1

- Fix some problems in the DDNS update code. Thanks to Albert Herranz for figuring out the main problem.
- Fix some reference counting errors on host entries that were causing core dumps.
- Fix a byte-swap bug in the token ring code, thanks to Jochen Friedrich.
- Fix a bug in lease billing, thanks to Jonas Bulow.

Changes since 3.0 Release Candidate 2

- Change the conditions under which a DHCPRELEASE is actually committed to be consistent with lease binding states rather than using the lease end time. This may fix some problems with the billing class code.

- Fix a bug where lease updates would fail on Digital Unix (and maybe others) because malloc was called with a size of zero.
- Fix a core dump that happens when the DHCP server can't create its trace file.

Changes since 3.0 Release Candidate 1 Patchlevel 1

- Fix the dhcp_failover_put_message to not attempt to allocate a zero-length buffer. Some versions of malloc() fail if you try to allocate a zero-length buffer, and this was causing problems on, e.g., Digital Unix.
- Fix a case where the failover code was printing an error message when no error had occurred.
- Fix a problem where when a server went down and back up again, the peer would not see a state transition and so would stay in the non-communicating state.
- Be smart about going into recover_wait.
- Fix a problem in the failover implementation where peers would fail to come into sync if interrupted in the RECOVER state. This could have been the cause of some problems people have reported recently.
- Fix a problem with billing classes where they would not be unbilled when the client lease expired.
- If select fails, figure out which descriptor is bad, and cut it out of the I/O loop. This prevents a potentially nasty spin. I haven't heard any report it in a while, but it came up consistently in testing.
- Fix a bug in the relay agent where if you specified interfaces on the command line, it would fail.
- Fix a couple of small bugs in the omapi connection object (no known user impact).
- Add the missing 3.0 Beta 1 lease conversion script.
- Read dhcp client script hooks if they exist, rather than only if they're executable.

Changes since 3.0 Release Candidate 1

- Fix a memory smash that happens when fixed-address leases are used. ANY SITE AT WHICH FIXED-ADDRESS STATEMENTS ARE BEING USED SHOULD UPGRADE IMMEDIATELY. This has been a long-standing bug - thanks to Alvise Nobile for discovering it and helping me to find it!
- Fix a small bug in binary-to-ascii, thanks to H. Peter Anvin of Transmeta.
- There is a known problem with the DHCP server doing failover on Compaq Alpha systems. This patchlevel is not a release candidate because of this bug. The bug should be straightforward to fix, so a new release candidate is expected shortly.
- There is a known problem in the DDNS update code that is probably a bug, and is not, as far as we know, fixed in this patchlevel.

Changes since 3.0 Beta 2 Patchlevel 24

- Went over problematic failover state transitions and made them all work, so that failover should now much less fragile.

- Add some dhcpctl and omapi documentation
- Fix compile errors when compiling with unusual predefines.
- Make Token Ring work on Linux 2.4
- Fix the Digital Unix BPF_WORDALIGN bug.
- Fix some dhcp client documentation errors.
- Update some parts of the README file.
- Support GCC on SCO.

Changes since 3.0 Beta 2 Patchlevel 23

- Fix a bug in the DNS update code where a status code was not being checked. This may have been causing core dumps.
- When parsing the lease file, if a lease declaration includes a billing class statement, and the lease already has a billing class, unbill the old class.
- When processing failover transactions, where acks will be deferred, process the state transition immediately.
- Don't try to use the new SIOCGIFCONF buffer size detection code on Linux 2.0, which doesn't provide this functionality.
- Apply a patch suggested by Tuan Uong for a problem in dlpi.c.
- Fix a problem in using the which command in the configure script.
- Fix a parse error in the client when setting up an omapi listener.
- Document the -n and -g flags to the client.
- Make sure there is always a stdin and stdout on startup. This prevents shell scripts from accidentally writing error messages into configuration files that happen to be opened as stderr.
- If an interface is removed, the client will now notice that it is gone rather than spinning. This has only been tested on NetBSD.
- The client will attempt to get an address even if it can't create a lease file.
- Don't overwrite tracefiles.
- Fix some memory allocation bugs in failover.

Changes since 3.0 Beta 2 Patchlevel 22

- Apply some patches suggested by Cyrille Lefevre, who is maintaining the FreeBSD ISC DHCP Distribution port.
- Fix a core dump in DHCPRELEASE.

Changes since 3.0 Beta 2 Patchlevel 21

- This time for sure: fix the spin described in the changes for pl20.

Changes since 3.0 Beta 2 Patchlevel 20

- Fix a problem with Linux detecting large numbers of interfaces (Ben)
- Fix a memory smash in the quotify code, which was introduced in

pl19.

- Actually fix the spin described in the changes for pl20. The previous fix only partially fixed the problem - enough to get it past the regression test.

Changes since 3.0 Beta 2 Patchlevel 19

- Fix a bug that could cause the server to abort if compiled with POINTER_DEBUG enabled.
- Fix a bug that could cause the server to spin when responding to a DHCPREQUEST.
- Apply Joost Mulders' suggested patches for DLPI on x86.
- Support NUL characters in quoted strings.
- Install unformatted man pages on SunOS.

Changes since 3.0 Beta 2 Patchlevel 18

- Allow the server to be placed in partner-down state using OMAPI. (Damien Neil)
- Implement omshell, which can be used to do arbitrary things to the server (in theory). (Damien Neil)
- Fix a case where if a client had two different leases the server could actually dereference the second one when it hadn't been referenced, leading to memory corruption and a core dump. (James Brister)
- Fix a case where a client could request the address of another client's lease, but find_lease wouldn't detect that the other client had it, and would attempt to allocate it to the client, resulting in a lease conflict message.
- Fix a case where a client with more than one client identifier could be given a lease where the hardware address was correct but the client identifier was not, resulting in a lease conflict message.
- Fix a problem where the server could write out a colon-separated hex list as a value for a variable, which would then not parse. The fix is to always write strings as quoted strings, with any non-printable characters quoted as octal escape sequences. So a file written the old way still won't work, but new files written this way will work.
- Fix documentation for sending non-standard options.
- Use unparseable names for unknown options. WARNING: this will break any configuration files that use the option-*nnn* convention. If you want to continue to use this convention for some options, please be sure to write a definition, like this:

```
option option-nnn code nnn = string;
```

You can use a descriptive name instead of option-*nnn* if you like.
- Fix a problem where we would see a DHCPDISCOVER/DHCP OFFER/DHCPREQUEST/DHCPACK/DHCPREQUEST/DHCPNAK sequence. This was the result of a deceptively silly bug in supersede_lease.
- Fix client script exit status check, according to a fix supplied by Hermann Lauer.
- Fix an endianness bug in the tracefile support, regarding ICMP messages.

- Fix a bug in the client where the medium would not work correctly if it contained quoted strings.

**** there was no pl17 ****

Changes since 3.0 Beta 2 Patchlevel 16

- Add support for transaction tracing. This allows the state of the DHCP server on startup, and all the subsequent transactions, to be recorded in a file which can then be played back to reproduce the behaviour of the DHCP server. This can be used to quickly reproduce bugs that cause core dumps or corruption, and also for tracking down memory leaks.
- Incorporate some bug fixes provided by Joost Mulders for the DLPI package which should clear up problems people have been seeing on Solaris.
- Fix bugs in the handling of options stored as linked lists (agent options, fqdn options and nwip options) that could cause memory corruption and core dumps.
- Fix a bug in DHCPREQUEST handling that resulted in DHCPNAK messages not being send in some cases when they were needed.
- Make the lease structure somewhat more compact.
- Make initial failover startup **much** faster. This was researched and implemented by Damien Neil.
- Add a `--version` flag to all executables, which prints the program name and version to standard output.
- Don't rewrite the lease file every thousand leases.
- A bug in nit.c for older SunOS machines was fixed by a patch sent in by Takeshi Hagiwara.
- Fix a memory corruption bug in the DHCP client.
- Lots of documentation updates.
- Add a feature allowing environment variables to be passed to the DHCP client script on the DHCP client command line.
- Fix client medium support, which had been broken for some time.
- Fix a bug in the DHCP client initial startup backoff interval, which would cause two DHCPDISCOVERS to be sent back-to-back on startup.

Changes since 3.0 Beta 2 Patchlevel 15

- Some documentation tweaks.
- Maybe fix a problem in the DLPI code.
- Fix some error code space inconsistencies in ddns update code.
- Support relay agents that intercept unicast DHCP messages to stuff agent options into them.
- Fix a small memory leak in the relay agent option support code.
- Fix a core dump that would occur if a packet was sent with no options.

Changes since 3.0 Beta 2 Patchlevel 14

- Finish fixing a long-standing bug in the agent options code. This was causing core dumps and failing to operate correctly - in particular, agent option stashing wasn't working. Agent option stashing should now be working, meaning that agent options can be used in class statements to control address allocation.
- Fix up documentation.
- Fix a couple of small memory leaks that would have added up significantly in a high-demand situation.
- Add a log-facility configuration parameter.
- Fix a compile error on some older operating systems.
- Add the ability in the client to execute certain statements before transmitting packets to the server. Handy for debugging; not much practical use otherwise.
- Don't send faked-out giaddr when renewing or bound - again, useful for debugging.

Changes since 3.0 Beta 2 Patchlevel 13

- Fixed a problem where the fqdn decoder would sometimes try to store an option with an (unsigned) negative length, resulting in a core dump on some systems.
- Work around the Win98 DHCP client, which NUL-terminates the FQDN option.
- Work around Win98 and Win2k clients that will claim they want to do the update even when they don't have any way to do it.
- Fix some log messages that can be printed when failover is operating that were not printing enough information.
- It was possible for a DHCPDISCOVER to get an allocation even when the state machine said the server shouldn't be responding.
- Don't load balance DHCPREQUESTs from clients in RENEWING and REBINDING, since in RENEWING, if we heard it, it's for us, and in REBINDING, the client wouldn't have got to REBINDING if its primary were answering.
- When we get a bogus state lease binding state transition, don't do the transition.

Changes since 3.0 Beta 2 Patchlevel 12

- Fixed a couple of silly compile errors.

Changes since 3.0 Beta 2 Patchlevel 11

- Albert Herranz tracked down and fixed a subtle bug in the base64 decoder that would prevent any key with an 'x' in its base64 representation from working correctly.
- Thanks to Chris Cheney and Michael Sanders, we have a fix for the hang that they both spotted in the DHCP server - when one-lease-per-client was set, the code to release the "other" lease could spin.
- Fix a problem with alignment of the input buffer in bpf in cases where two packets arrive in the same bpf read.

- Fix a problem where the relay agent would crash if you specified an interface name on the command line.
- Add the ability to conditionalize client behaviour based on the client state.
- Add support for the FQDN option, and added support for a new way of doing ddns updates (ddns update style interim) that allows more than one DHCP server to update the DNS for the same network(s). This was implemented by Damien Neil with some additional functionality added by Ted Lemon.
- Damien added a "log" statement, so that the configuration file can be made to log debugging information and other information.
- Fixed a bug that caused option buffers not to be terminated with an end option.
- Fixed a long-standing bug in the support for option spaces where the options are stored as an ordered list rather than in a hash table, which could theoretically result in memory pool corruption.
- Prevent hardware declarations with no actual hardware address from being written as something unparsable, and behave correctly in the face of a null hardware address on input.
- Allow key names to be FQDNs, and qualify the algorithm name if it is specified unqualified.
- Modify the DDNS update code so that it never prints the "resolver failed" message, but instead says *why* the resolver failed.
- Officially support the subnet selection option, which now has an RFC.
- Fix a build bug on MacOS X.
- Allow administrator to disable ping checking.
- Clean up dhcpd.conf documentation and add more information about how it works.

Changes since 3.0 Beta 2 Patchlevel 10

- Fix a bug introduced during debugging (!) and accidentally committed to CVS.

Changes since 3.0 Beta 2 Patchlevel 9

- Fix DHCP client handling of vendor encapsulated options.
- Fix a bug in the handling of relay agent information options introduced in patchlevel 9.
- Stash agent options on client leases by default, and use the stashed options at renewal time.
- Add the ability to test the client's binding state in the client configuration language.
- Fix a core dump in the DNS update code.
- Fix some expression evaluation bugs that were causing updates to be done when no client hostname was received.
- Fix expression evaluation debugging printf's.
- Teach pretty_print_option to print options in option spaces other than

the DHCP option space.

- Add a warning message if the RHS of a not is not boolean.
- Never select for more than a day, because some implementations of select will just fail if the timeout is too long (!).
- Fix a case where a DHCPDISCOVER from an unknown network would be silently dropped.
- Fix a bug where if a client requested an IP address for which a different client had the lease, the DHCP server would reallocate it anyway.
- Fix the DNS update code so that if the client changes its name, the DNS will be correctly updated.

Changes since 3.0 Beta 2 Patchlevel 8

- Oops, there was another subtle math error in the header-length bounds-checking.

Changes since 3.0 Beta 2 Patchlevel 7

- Oops, forgot to byte-swap udp header length before bounds-checking it.

Changes since 3.0 Beta 2 Patchlevel 6

- Fix a possible DoS attack where a client could cause the checksummer to dump core. This was a read, not a write, so it shouldn't be possible to exploit it any further than that.
- Implement client- and server-side support for using the Client FQDN option.
- Support for other option spaces in the client has been added. This means that it is now possible to define a vendor option space on the client, request options in that space from the server (which must define the same option space), and then use those options in the client. This also allows NWIP and Client FQDN options to be used meaningfully.
- Add object initializer support. This means that objects can now be initialized to something other than all-zeros when allocated, which makes, e.g., the interface object support code a little more robust.
- Fix an off-by-one bug in the host stuffer. This was causing host deletes not the work, and may also have been causing OMAPI connections to get dropped. Thanks to James Brister for tracking this one down!
- Fixed a core dump in the interface discovery code that is triggered when there is no subnet declaration for an interface, but the server decides to continue running. Thanks to Shane Kerr for tracking down and fixing this problem.

Changes since 3.0 Beta 2 Patchlevel 5

- Fix a bug in the recent enhancement to the interface discovery code to support arbitrary-length interface lists.
- Support NUL-terminated DHCP options when initializing client-script environment.
- Fix suffix operator.
- Fix NetWare/IP option parsing.
- Better error/status checking in dhcpcctl initialization and omapi

connection code.

- Fix a potential memory smash in dhcpctl code.
- Fix SunOS4 and (maybe) Ultrix builds.
- Fix a bug where a certain sort of incoming packet could cause a core dump on Solaris (and probably elsewhere).
- Add some more safety checks in error logging code.
- Add support for ISC_R_INCOMPLETE in OMAPI protocol connection code.
- Fix relay agent so that if an interface is specified on the command line, the relay agent does not dump core.
- Fix class matching so that match if can be combined with match or spawn with.
- Do not allow spurious leases in the lease database to introduce potentially bogus leases into the in-memory database.
- Fix a byte-order problem in the client hardware address type code for OMAPI.
- Be slightly less picky about what sort of hardware addresses OMAPI can install in host declarations.

Changes since 3.0 Beta 2 Patchlevel 4

- Incorporated Peter Marschall's proposed change to array/record parsing, which allows things like the slp-agent option to be encoded correctly. Thanks very much to Peter for taking the initiative to do this, and for doing such a careful job of it (e.g., updating the comments)!
- Added an encoding for the slp-agent option. :')
- Fixed SunOS 4 build. Thanks to Robert Elz for responding to my request for help on this with patches!
- Incorporated a change that should fix a problem reported by Philippe Jumelle where when the network connection between two servers is lost, they never reconnect.
- Fix client script files other than that for NetBSD to actually use make_resolv_conf as documented in the manual page.
- Fix a bug in the packet handling code that could result in a core dump.
- Fix a bug in the bootp code where responses on the local net would be sent to the wrong MAC address. Thanks to Jerry Schave for catching this one.

Changes since 3.0 Beta 2 Patchlevel 3

- In the DHCP client, execute client statements prior to using the values of options, so that the client configuration can be overridden, e.g., the lease renewal time.
- Fix a reference counting error that would result in very reproducible failures in updates, as well as occasional core dumps, if a zone was declared without a key.
- Fix some Linux 2.0 compilation problems.
- Fix a bug in scope evaluation during execution of "on" statements that

caused values not to be recorded on leases.

- If the dhcp-max-message-size option is specified in scope, and the client didn't send this option, use the one specified in scope to determine the maximum size of the response.

Changes since 3.0 Beta 2 Patchlevel 2

- Fix a case where spawning subclasses were being allocated incorrectly, resulting in a core dump.
- Fix a case where the DHCP server might inappropriately NAK a RENEWING client.
- Fix a place dhcprequest() where static leases could leak.
- Include memory.h in omapip_p.h so that we don't get warnings about using memcmp().

Changes since 3.0 Beta 2 Patchlevel 1

- Notice when SIOCFIGCONF returns more data than fit in the buffer - allocate a larger buffer, and retry. Thanks to Greg Fausak for pointing this out.
- In the server, if no interfaces were configured, report an error and exit.
- Don't ever record a state of 'startup'.
- Don't try to evaluate the local failover binding address if none was specified. Thanks to Joseph Breu for finding this.