```
**********************************************************
   35272 Sat May 10 16:17:41 2014
new/usr/src/lib/libnsl/rpc/rpcb_clnt.c
4729 __rpcb_findaddr_timed should try rpcbind protocol 4 first
**********************************************************
```

```
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License, Version 1.0 only
 * (the "License").  You may not use this file except in compliance
 * with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */

/*
 * Copyright 2014 Gary Mills
 * Copyright 2006 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

/* Copyright (c) 1983, 1984, 1985, 1986, 1987, 1988, 1989 AT&T */
/* All Rights Reserved */
/*
 * Portions of this source code were derived from Berkeley
 * 4.3 BSD under license from the Regents of the University of
 * California.
 */

#pragma ident   "%Z%%M% %I%     %E% SMI"

/*
 * interface to rpcbind rpc service.
 */

#include "mt.h"
#include "rpc_mt.h"
#include <assert.h>
#include <rpc/rpc.h>
#include <rpc/rpcb_prot.h>
#include <netconfig.h>
#include <netdir.h>
#include <rpc/nettype.h>
#include <syslog.h>
#ifdef PORTMAP
#include <netinet/in.h>         /* FOR IPPROTO_TCP/UDP definitions */
#include <rpc/pmap_prot.h>
#endif
#ifdef ND_DEBUG
#include <stdio.h>
#endif
#include <sys/utsname.h>
#include <errno.h>
#include <stdlib.h>
```



```
#include <string.h>
#include <unistd.h>

static struct timeval tottimeout = { 60, 0 };
static const struct timeval rmttimeout = { 3, 0 };
static struct timeval rpcbrmttime = { 15, 0 };

extern bool_t xdr_wrapstring(XDR *, char **);

static const char nullstring[] = "\000";

extern CLIENT *_clnt_tli_create_timed(int, const struct netconfig *,
                        struct netbuf *, rpcprog_t, rpcvers_t, uint_t, uint_t,
                        const struct timeval *);

static CLIENT *_getclnthandle_timed(char *, struct netconfig *, char **,
                        struct timeval *);


/*
 * The life time of a cached entry should not exceed 5 minutes
 * since automountd attempts an unmount every 5 minutes.
 * It is arbitrarily set a little lower (3 min = 180 sec)
 * to reduce the time during which an entry is stale.
 */
#define CACHE_TTL 180
#define CACHESIZE 6

struct address_cache {
        char *ac_host;
        char *ac_netid;
        char *ac_uaddr;
        struct netbuf *ac_taddr;
        struct address_cache *ac_next;
        time_t ac_maxtime;
};
_____unchanged_portion_omitted_

/*
 *      It might seem that a reader/writer lock would be more reasonable here.
 *      However because getclnthandle(), the only user of the cache functions,
 *      may do a delete_cache() operation if a check_cache() fails to return an
 *      address useful to clnt_tli_create(), we may as well use a mutex.
 */
/*
 * As it turns out, if the cache lock is *not* a reader/writer lock, we will
 * block all clnt_create's if we are trying to connect to a host that's down,
 * since the lock will be held all during that time.
 */
extern rwlock_t rpcbaddr_cache_lock;

/*
 * The routines check_cache(), add_cache(), delete_cache() manage the
 * cache of rpcbind addresses for (host, netid).
 */

static struct address_cache *
check_cache(char *host, char *netid)
{
        struct address_cache *cptr;

        /* READ LOCK HELD ON ENTRY: rpcbaddr_cache_lock */

        assert(RW_READ_HELD(&rpcbaddr_cache_lock));
        for (cptr = front; cptr != NULL; cptr = cptr->ac_next) {
                if ((strcmp(cptr->ac_host, host) == 0) &&
```

```
                    (strcmp(cptr->ac_netid, netid) == 0) &&
                    (time(NULL) <= cptr->ac_maxtime)) {
#ifdef ND_DEBUG
                        fprintf(stderr, "Found cache entry for %s: %s\n",
                                host, netid);
#endif
                        return (cptr);
                }
        }
        return (NULL);
}
```

*unchanged_portion_omitted_*

```
static void
add_cache(char *host, char *netid, struct netbuf *taddr, char *uaddr)
{
        struct address_cache  *ad_cache, *cptr, *prevptr;

        ad_cache = malloc(sizeof (struct address_cache));
        if (!ad_cache) {
                goto memerr;
        }
        ad_cache->ac_maxtime = time(NULL) + CACHE_TTL;
        ad_cache->ac_host = strdup(host);
        ad_cache->ac_netid = strdup(netid);
        ad_cache->ac_uaddr = uaddr ? strdup(uaddr) : NULL;
        ad_cache->ac_taddr = malloc(sizeof (struct netbuf));
        if (!ad_cache->ac_host || !ad_cache->ac_netid || !ad_cache->ac_taddr ||
            (uaddr && !ad_cache->ac_uaddr)) {
                goto memerr1;
        }

        ad_cache->ac_taddr->len = ad_cache->ac_taddr->maxlen = taddr->len;
        ad_cache->ac_taddr->buf = malloc(taddr->len);
        if (ad_cache->ac_taddr->buf == NULL) {
                goto memerr1;
        }

        (void) memcpy(ad_cache->ac_taddr->buf, taddr->buf, taddr->len);
#ifdef ND_DEBUG
        (void) fprintf(stderr, "Added to cache: %s : %s\n", host, netid);
#endif

/* VARIABLES PROTECTED BY rpcbaddr_cache_lock:  cptr */

        (void) rw_wrlock(&rpcbaddr_cache_lock);
        if (cachesize < CACHESIZE) {
                ad_cache->ac_next = front;
                front = ad_cache;
                cachesize++;
        } else {
                /* Free the last entry */
                cptr = front;
                prevptr = NULL;
                while (cptr->ac_next) {
                        prevptr = cptr;
                        cptr = cptr->ac_next;
                }

#ifdef ND_DEBUG
                fprintf(stderr, "Deleted from cache: %s : %s\n",
                        cptr->ac_host, cptr->ac_netid);
#endif
                free(cptr->ac_host);
                free(cptr->ac_netid);
                free(cptr->ac_taddr->buf);
```



```
                free(cptr->ac_taddr);
                if (cptr->ac_uaddr)
                        free(cptr->ac_uaddr);

                if (prevptr) {
                        prevptr->ac_next = NULL;
                        ad_cache->ac_next = front;
                        front = ad_cache;
                } else {
                        front = ad_cache;
                        ad_cache->ac_next = NULL;
                }
                free(cptr);
        }
        (void) rw_unlock(&rpcbaddr_cache_lock);
        return;
memerr1:
        if (ad_cache->ac_host)
                free(ad_cache->ac_host);
        if (ad_cache->ac_netid)
                free(ad_cache->ac_netid);
        if (ad_cache->ac_uaddr)
                free(ad_cache->ac_uaddr);
        if (ad_cache->ac_taddr)
                free(ad_cache->ac_taddr);
        free(ad_cache);
memerr:
        syslog(LOG_ERR, "add_cache : out of memory.");
}
```

*unchanged_portion_omitted_*

```
/*
 * Same as getclnthandle() except it takes an extra timeout argument.
 * This is for bug 4049792: clnt_create_timed does not timeout.
 *
 * If tp is NULL, use default timeout to get a client handle.
 */
static CLIENT *
_getclnthandle_timed(char *host, struct netconfig *nconf, char **targaddr,
                                                        struct timeval *tp)
{
        CLIENT *client = NULL;
        struct netbuf *addr;
        struct netbuf addr_to_delete;
        struct nd_addrlist *nas;
        struct nd_hostserv rpcbind_hs;
        struct address_cache *ad_cache;
        char *tmpaddr;
        int neterr;
        int j;

/* VARIABLES PROTECTED BY rpcbaddr_cache_lock:  ad_cache */

        /* Get the address of the rpcbind.  Check cache first */
        addr_to_delete.len = 0;
        (void) rw_rdlock(&rpcbaddr_cache_lock);
        ad_cache = check_cache(host, nconf->nc_netid);
        if (ad_cache != NULL) {
                addr = ad_cache->ac_taddr;
                client = _clnt_tli_create_timed(RPC_ANYFD, nconf, addr,
                    RPCBPROG, RPCBVERS4, 0, 0, tp);
                if (client != NULL) {
                        if (targaddr) {
                                /*
                                 * case where a client handle is created
                                 * without a targaddr and the handle is
```

```
323                                  * requested with a targaddr
324                                  */
325                                 if (ad_cache->ac_uaddr != NULL) {
326                                         *targaddr = strdup(ad_cache->ac_uaddr);
327                                         if (*targaddr == NULL) {
328                                                 syslog(LOG_ERR,
329                                                 "_getclnthandle_timed: strdup "
330                                                 "failed.");
331                                                 rpc_createerr.cf_stat =
332                                                     RPC_SYSTEMERROR;
333                                                 (void) rw_unlock(
334                                                     &rpcbaddr_cache_lock);
335                                                 return (NULL);
336                                         }
337                                 } else {
338                                         *targaddr = NULL;
339                                 }
340                         }
341                         (void) rw_unlock(&rpcbaddr_cache_lock);
342                         return (client);
343                 }
344                 if (rpc_createerr.cf_stat == RPC_SYSTEMERROR) {
345                         (void) rw_unlock(&rpcbaddr_cache_lock);
346                         return (NULL);
347                 }
348                 addr_to_delete.len = addr->len;
349                 addr_to_delete.buf = malloc(addr->len);
350                 if (addr_to_delete.buf == NULL) {
351                         addr_to_delete.len = 0;
352                 } else {
353                         (void) memcpy(addr_to_delete.buf, addr->buf, addr->len);
354                 }
355         }
356         (void) rw_unlock(&rpcbaddr_cache_lock);
357         if (addr_to_delete.len != 0) {
358                 /*
359                  * Assume this may be due to cache data being
360                  *  outdated
361                  */
362                 (void) rw_wrlock(&rpcbaddr_cache_lock);
363                 delete_cache(&addr_to_delete);
364                 (void) rw_unlock(&rpcbaddr_cache_lock);
365                 free(addr_to_delete.buf);
366         }
367         rpcbind_hs.h_host = host;
368         rpcbind_hs.h_serv = "rpcbind";
384 #ifdef ND_DEBUG
385         fprintf(stderr, "rpcbind client routines: diagnostics :\n");
386         fprintf(stderr, "\tGetting address for (%s, %s, %s) ... \n",
387                 rpcbind_hs.h_host, rpcbind_hs.h_serv, nconf->nc_netid);
388 #endif

370         if ((neterr = netdir_getbyname(nconf, &rpcbind_hs, &nas)) != 0) {
371                 if (neterr == ND_NOHOST)
372                         rpc_createerr.cf_stat = RPC_UNKNOWNHOST;
373                 else
374                         rpc_createerr.cf_stat = RPC_N2AXLATEFAILURE;
375                 return (NULL);
376         }
377         /* XXX nas should perhaps be cached for better performance */

379         for (j = 0; j < nas->n_cnt; j++) {
380                 addr = &(nas->n_addrs[j]);
401 #ifdef ND_DEBUG
402 {
403         int i;
```



```
404         char *ua;

406         ua = taddr2uaddr(nconf, &(nas->n_addrs[j]));
407         fprintf(stderr, "Got it [%s]\n", ua);
408         free(ua);

410         fprintf(stderr, "\tnetbuf len = %d, maxlen = %d\n",
411                 addr->len, addr->maxlen);
412         fprintf(stderr, "\tAddress is ");
413         for (i = 0; i < addr->len; i++)
414                 fprintf(stderr, "%u.", addr->buf[i]);
415         fprintf(stderr, "\n");
416 }
417 #endif
381         client = _clnt_tli_create_timed(RPC_ANYFD, nconf, addr, RPCBPROG,
382             RPCBVERS4, 0, 0, tp);
383         if (client)
384                 break;
385         }
423 #ifdef ND_DEBUG
424         if (!client) {
425                 clnt_pcreateerror("rpcbind clnt interface");
426         }
427 #endif

387         if (client) {
388                 tmpaddr = targaddr ? taddr2uaddr(nconf, addr) : NULL;
389                 add_cache(host, nconf->nc_netid, addr, tmpaddr);
390                 if (targaddr) {
391                         *targaddr = tmpaddr;
392                 }
393         }
394         netdir_free((char *)nas, ND_ADDRLIST);
395         return (client);
396 }

398 /*
399  * This routine will return a client handle that is connected to the local
400  * rpcbind. Returns NULL on error.
442  * rpcbind. Returns NULL on error and free's everything.
401  */
402 static CLIENT *
403 local_rpcb(void)
404 {
405         static struct netconfig *loopnconf;
406         static char *hostname;
407         extern mutex_t loopnconf_lock;

409 /* VARIABLES PROTECTED BY loopnconf_lock: hostname loopnconf */
451 /* VARIABLES PROTECTED BY loopnconf_lock: loopnconf */
410         (void) mutex_lock(&loopnconf_lock);
411         if (loopnconf == NULL) {
412                 struct utsname utsname;
413                 struct netconfig *nconf, *tmpnconf = NULL;
414                 void *nc_handle;

416                 if (hostname == NULL) {
417 #if defined(__i386) && !defined(__amd64)
418                         if ((_nuname(&utsname) == -1) ||
419                             ((hostname = strdup(utsname.nodename)) == NULL)) {
420 #else
421                         if ((uname(&utsname) == -1) ||
422                             ((hostname = strdup(utsname.nodename)) == NULL)) {
423 #endif
464                             ((hostname = strdup(utsname.nodename)) == NULL)) {
424                                 syslog(LOG_ERR, "local_rpcb : strdup failed.");
```

```
425                                 rpc_createerr.cf_stat = RPC_UNKNOWNHOST;
426                                 (void) mutex_unlock(&loopnconf_lock);
427                                 return (NULL);
428                         }
429                         /* hostname is never freed */
430                 }
431                 nc_handle = setnetconfig();
432                 if (nc_handle == NULL) {
433                         /* fails to open netconfig file */
434                         rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
435                         (void) mutex_unlock(&loopnconf_lock);
436                         return (NULL);
437                 }
438                 while (nconf = getnetconfig(nc_handle)) {
439                         if (strcmp(nconf->nc_protofmly, NC_LOOPBACK) == 0) {
440                                 tmpnconf = nconf;
441                                 if (nconf->nc_semantics == NC_TPI_CLTS)
442                                         break;
443                         }
444                 }
445                 if (tmpnconf == NULL) {
446                         rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
447                         (void) mutex_unlock(&loopnconf_lock);
448                         return (NULL);
449                 }
450                 loopnconf = getnetconfigent(tmpnconf->nc_netid);
451                 /* loopnconf is never freed */
452                 (void) endnetconfig(nc_handle);
453         }
454         (void) mutex_unlock(&loopnconf_lock);
455         return (getclnthandle(hostname, loopnconf, NULL));
456 }
```

unchanged_portion_omitted_

```
545 /*
546  * From the merged list, find the appropriate entry
547  */
548 static struct netbuf *
549 got_entry(rpcb_entry_list_ptr relp, struct netconfig *nconf)
550 {
551         struct netbuf *na = NULL;
552         rpcb_entry_list_ptr sp;
553         rpcb_entry *rmap;

555         for (sp = relp; sp != NULL; sp = sp->rpcb_entry_next) {
556                 rmap = &sp->rpcb_entry_map;
557                 if ((strcmp(nconf->nc_proto, rmap->r_nc_proto) == 0) &&
558                     (strcmp(nconf->nc_protofmly, rmap->r_nc_protofmly) == 0) &&
559                     (nconf->nc_semantics == rmap->r_nc_semantics) &&
560                     (rmap->r_maddr != NULL) && (rmap->r_maddr[0] != NULL)) {
561                         na = uaddr2taddr(nconf, rmap->r_maddr);
562 #ifdef ND_DEBUG
603                         fprintf(stderr, "\tRemote address is [%s].\n",
604                                 rmap->r_maddr);
605                         if (!na)
606                                 fprintf(stderr,
607                                     "\tCouldn't resolve remote address!\n");
608 #endif
562                         break;
563                 }
564         }
565         return (na);
566 }
```

unchanged_portion_omitted_


```
641 /*
642  * An internal function which optimizes rpcb_getaddr function.  It returns
643  * the universal address of the remote service or NULL.  It also optionally
689  * An internal function which optimizes rpcb_getaddr function.  It also
644  * returns the client handle that it uses to contact the remote rpcbind.
645  * The caller will re-purpose the client to contact the remote service.
646  *
647  * The algorithm used: First try version 4.  Then try version 3 (svr4).
648  * Finally, if the transport is TCP or UDP, try version 2 (portmap).
649  * Version 4 is now available with all current systems on the network.
692  * The algorithm used: If the transports is TCP or UDP, it first tries
693  * version 2 (portmap), 4 and then 3 (svr4).  This order should be
694  * changed in the next OS release to 4, 2 and 3.  We are assuming that by
695  * that time, version 4 would be available on many machines on the network.
650  * With this algorithm, we get performance as well as a plan for
651  * obsoleting version 2.
652  *
699  * For all other transports, the algorithm remains as 4 and then 3.
700  *
653  * XXX: Due to some problems with t_connect(), we do not reuse the same client
654  * handle for COTS cases and hence in these cases we do not return the
655  * client handle.  This code will change if t_connect() ever
656  * starts working properly.  Also look under clnt_vc.c.
657  */
658 struct netbuf *
659 __rpcb_findaddr_timed(rpcprog_t program, rpcvers_t version,
660         struct netconfig *nconf, char *host, CLIENT **clpp, struct timeval *tp)
661 {
662         static bool_t check_rpcbind = TRUE;
663         CLIENT *client = NULL;
664         RPCB parms;
665         enum clnt_stat clnt_st;
666         char *ua = NULL;
667         uint_t vers;
668         struct netbuf *address = NULL;
669         void *handle;
670         rpcb_entry_list_ptr relp = NULL;
671         bool_t tmp_client = FALSE;
717         uint_t start_vers = RPCBVERS4;

673         /* parameter checking */
674         if (nconf == NULL) {
675                 rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
676                 return (NULL);
677         }

679         parms.r_addr = NULL;

681         /*
682          * Use default total timeout if no timeout is specified.
683          */
684         if (tp == NULL)
685                 tp = &tottimeout;

733 #ifdef PORTMAP
734         /* Try version 2 for TCP or UDP */
735         if (strcmp(nconf->nc_protofmly, NC_INET) == 0) {
736                 ushort_t port = 0;
737                 struct netbuf remote;
738                 uint_t pmapvers = 2;
739                 struct pmap pmapparms;

687         /*
742                  * Try UDP only - there are some portmappers out
743                  * there that use UDP only.
744                  */
```

```
745                 if (strcmp(nconf->nc_proto, NC_TCP) == 0) {
746                         struct netconfig *newnconf;
747                         void *handle;

749                         if ((handle = __rpc_setconf("udp")) == NULL) {
750                                 rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
751                                 return (NULL);
752                         }

754                         /*
755                          * The following to reinforce that you can
756                          * only request for remote address through
757                          * the same transport you are requesting.
758                          * ie. requesting unversial address
759                          * of IPv4 has to be carried through IPv4.
760                          * Can't use IPv6 to send out the request.
761                          * The mergeaddr in rpcbind can't handle
762                          * this.
763                          */
764                         for (;;) {
765                                 if ((newnconf = __rpc_getconf(handle))
766                                                                 == NULL) {
767                                         __rpc_endconf(handle);
768                                         rpc_createerr.cf_stat =
769                                             RPC_UNKNOWNPROTO;
770                                         return (NULL);
771                                 }
772                                 /*
773                                  * here check the protocol family to
774                                  * be consistent with the request one
775                                  */
776                                 if (strcmp(newnconf->nc_protofmly,
777                                     nconf->nc_protofmly) == NULL)
778                                         break;
779                         }

781                         client = _getclnthandle_timed(host, newnconf,
782                                         &parms.r_addr, tp);
783                         __rpc_endconf(handle);
784                 } else {
785                         client = _getclnthandle_timed(host, nconf,
786                                         &parms.r_addr, tp);
787                 }
788                 if (client == NULL)
789                         return (NULL);

791                 /*
792                  * Set version and retry timeout.
793                  */
794                 CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT, (char *)&rpcbrmttime);
795                 CLNT_CONTROL(client, CLSET_VERS, (char *)&pmapvers);

797                 pmapparms.pm_prog = program;
798                 pmapparms.pm_vers = version;
799                 pmapparms.pm_prot = strcmp(nconf->nc_proto, NC_TCP) ?
800                                     IPPROTO_UDP : IPPROTO_TCP;
801                 pmapparms.pm_port = 0;  /* not needed */
802                 clnt_st = CLNT_CALL(client, PMAPPROC_GETPORT,
803                                     (xdrproc_t)xdr_pmap, (caddr_t)&pmapparms,
804                                     (xdrproc_t)xdr_u_short, (caddr_t)&port,
805                                     *tp);
806                 if (clnt_st != RPC_SUCCESS) {
807                         if ((clnt_st == RPC_PROGVERSMISMATCH) ||
808                             (clnt_st == RPC_PROGUNAVAIL))
809                                 goto try_rpcbind; /* Try different versions */
810                         rpc_createerr.cf_stat = RPC_PMAPFAILURE;
```



```
811                         clnt_geterr(client, &rpc_createerr.cf_error);
812                         goto error;
813                 } else if (port == 0) {
814                         address = NULL;
815                         rpc_createerr.cf_stat = RPC_PROGNOTREGISTERED;
816                         goto error;
817                 }
818                 port = htons(port);
819                 CLNT_CONTROL(client, CLGET_SVC_ADDR, (char *)&remote);
820                 if (((address = malloc(sizeof (struct netbuf))) == NULL) ||
821                     ((address->buf = malloc(remote.len)) == NULL)) {
822                         rpc_createerr.cf_stat = RPC_SYSTEMERROR;
823                         clnt_geterr(client, &rpc_createerr.cf_error);
824                         if (address) {
825                                 free(address);
826                                 address = NULL;
827                         }
828                         goto error;
829                 }
830                 (void) memcpy(address->buf, remote.buf, remote.len);
831                 (void) memcpy(&address->buf[sizeof (short)], &port,
832                                                         sizeof (short));
833                 address->len = address->maxlen = remote.len;
834                 goto done;
835         }
836 #endif

838 try_rpcbind:
839         /*
688          * Check if rpcbind is up.  This prevents needless delays when
689          * accessing applications such as the keyserver while booting
690          * disklessly.
691          */
692         if (check_rpcbind && strcmp(nconf->nc_protofmly, NC_LOOPBACK) == 0) {
693                 if (!__rpcbind_is_up()) {
694                         rpc_createerr.cf_stat = RPC_PMAPFAILURE;
695                         rpc_createerr.cf_error.re_errno = 0;
696                         rpc_createerr.cf_error.re_terrno = 0;
697                         goto error;
698                 }
699                 check_rpcbind = FALSE;
700         }

702         /*
703          * First try version 4.
855          * Now we try version 4 and then 3.
856          * We also send the remote system the address we used to
857          * contact it in case it can help to connect back with us
704          */
705         parms.r_prog = program;
706         parms.r_vers = version;
707         parms.r_owner = (char *)&nullstring[0]; /* not needed; */
708         /* just for xdring */
709         parms.r_netid = nconf->nc_netid; /* not really needed */

711         /*
712          * If a COTS transport is being used, try getting address via CLTS
713          * transport.  This works only with version 4.
714          */
715         if (nconf->nc_semantics == NC_TPI_COTS_ORD ||
716             nconf->nc_semantics == NC_TPI_COTS) {
717                 tmp_client = TRUE;
718                 if ((handle = __rpc_setconf("datagram_v")) != NULL) {
871                 void *handle;
719                         struct netconfig *nconf_clts;
873                 rpcb_entry_list_ptr relp = NULL;
```

```
721                         while ((nconf_clts = __rpc_getconf(handle)) != NULL) {
875                 if (client == NULL) {
876                         /* This did not go through the above PORTMAP/TCP code */
877                         if ((handle = __rpc_setconf("datagram_v")) != NULL) {
878                                 while ((nconf_clts = __rpc_getconf(handle))
879                                     != NULL) {
722                                 if (strcmp(nconf_clts->nc_protofmly,
723                                     nconf->nc_protofmly) != 0) {
724                                         continue;
725                                 }
726                                 client = _getclnthandle_timed(host, nconf_clts,
727                                     &parms.r_addr, tp);
884                                         client = _getclnthandle_timed(host,
885                                                 nconf_clts, &parms.r_addr,
886                                                 tp);
728                                 break;
729                         }
730                         __rpc_endconf(handle);
731                 }
891                         if (client == NULL)
892                                 goto regular_rpcbind;   /* Go the regular way */
732         } else {
733                 client = _getclnthandle_timed(host, nconf, &parms.r_addr, tp);
734                 /* Sets cf_error members on failure */
735         }

737         if (client != NULL) {

739                 /* Set rpcbind version 4 */
894                         /* This is a UDP PORTMAP handle.  Change to version 4 */
740                 vers = RPCBVERS4;
741                 CLNT_CONTROL(client, CLSET_VERS, (char *)&vers);

897                 }
743                 /*
744                  * We also send the remote system the address we used to
745                  * contact it in case it can help it connect back with us
746                  */
747                 if (parms.r_addr == NULL) {
748                         parms.r_addr = strdup(""); /* for XDRing */
749                         if (parms.r_addr == NULL) {
750                                 syslog(LOG_ERR, "__rpcb_findaddr_timed: "
751                                     "strdup failed.");
752                                 /* cf_error is still zeroed */
753                                 rpc_createerr.cf_error.re_errno = errno;
754                                 rpc_createerr.cf_stat = RPC_SYSTEMERROR;
908                                 address = NULL;
755                                 goto error;
756                         }
757                 }

759                 CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT,
760                     (char *)&rpcbrmttime);
913                 CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT, (char *)&rpcbrmttime);

762                 clnt_st = CLNT_CALL(client, RPCBPROC_GETADDRLIST,
763                     (xdrproc_t)xdr_rpcb, (char *)&parms,
764                     (xdrproc_t)xdr_rpcb_entry_list_ptr, (char *)&relp, *tp);
765                 /* Sets error structure members in client handle */
766                 switch (clnt_st) {
767                 case RPC_SUCCESS: /* Call succeeded */
768                         address = got_entry(relp, nconf);
917                                 (xdrproc_t)xdr_rpcb_entry_list_ptr,
918                                 (char *)&relp, *tp);
919                 if (clnt_st == RPC_SUCCESS) {
```



```
920                         if (address = got_entry(relp, nconf)) {
769                         xdr_free((xdrproc_t)xdr_rpcb_entry_list_ptr,
770                             (char *)&relp);
771                         if (address != NULL) {
772                                 /* Program number and version number matched */
773                                 goto done;
774                         }
775                         /* Program and version not found for this transport */
925                         /* Entry not found for this transport */
926                         xdr_free((xdrproc_t)xdr_rpcb_entry_list_ptr,
927                                 (char *)&relp);
776                         /*
777                          * XXX: should have returned with RPC_PROGUNAVAIL
778                          * or perhaps RPC_PROGNOTREGISTERED error but
929                          * XXX: should have perhaps returned with error but
779                          * since the remote machine might not always be able
780                          * to send the address on all transports, we try the
781                          * regular way with version 3, then 2
932                          * regular way with regular_rpcbind
782                          */
783                         /* Try the next version */
784                         break;
785                 case RPC_PROGVERSMISMATCH: /* RPC protocol mismatch */
786                         clnt_geterr(client, &rpc_createerr.cf_error);
787                         if (rpc_createerr.cf_error.re_vers.low > vers) {
788                                 rpc_createerr.cf_stat = clnt_st;
789                                 goto error;  /* a new version, can't handle */
790                         }
791                         /* Try the next version */
792                         break;
793                 case RPC_PROCUNAVAIL: /* Procedure unavailable */
794                 case RPC_PROGUNAVAIL: /* Program not available */
795                 case RPC_TIMEDOUT: /* Call timed out */
796                         /* Try the next version */
797                         break;
798                 default:
799                         clnt_geterr(client, &rpc_createerr.cf_error);
934                         goto regular_rpcbind;
935                 } else if ((clnt_st == RPC_PROGVERSMISMATCH) ||
936                             (clnt_st == RPC_PROGUNAVAIL)) {
937                         start_vers = RPCBVERS;  /* Try version 3 now */
938                         goto regular_rpcbind; /* Try different versions */
939                 } else {
800                         rpc_createerr.cf_stat = RPC_PMAPFAILURE;
941                         clnt_geterr(client, &rpc_createerr.cf_error);
801                         goto error;
802                         break;
803                 }
944         }

805         } else {
946 regular_rpcbind:

807                 /* No client */
808                 tmp_client = FALSE;

810         } /* End of version 4 */

812         /* Destroy a temporary client */
813         if (client != NULL && tmp_client) {
948         /* Now the same transport is to be used to get the address */
949         if (client && ((nconf->nc_semantics == NC_TPI_COTS_ORD) ||
950             (nconf->nc_semantics == NC_TPI_COTS))) {
951                 /* A CLTS type of client - destroy it */
814                 CLNT_DESTROY(client);
815                 client = NULL;
```

```
816                 free(parms.r_addr);
817                 parms.r_addr = NULL;
818         }
819         tmp_client = FALSE;

821         /*
822          * Try version 3
823          */

825         /* Now the same transport is to be used to get the address */
826         if (client == NULL) {
827                 client = _getclnthandle_timed(host, nconf, &parms.r_addr, tp);
828                 /* Sets cf_error members on failure */
829         }
960                 if (client == NULL) {
830         address = NULL;
831         if (client != NULL) {
962                         goto error;
963                 }
964         }
832                 if (parms.r_addr == NULL) {
833                         parms.r_addr = strdup("");      /* for XDRing */
834                         if (parms.r_addr == NULL) {
835                                 syslog(LOG_ERR, "__rpcb_findaddr_timed: "
836                                     "strdup failed.");
837                                 /* cf_error is still zeroed */
838                                 rpc_createerr.cf_error.re_errno = errno;
970                         address = NULL;
839                                 rpc_createerr.cf_stat = RPC_SYSTEMERROR;
840                                 goto error;
841                         }
842                 }

844                 CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT,
845                     (char *)&rpcbrmttime);
846                 vers = RPCBVERS; /* Set the version */
976         /* First try from start_vers and then version 3 (RPCBVERS) */

978         CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT, (char *)&rpcbrmttime);
979         for (vers = start_vers;  vers >= RPCBVERS; vers--) {
980                 /* Set the version */
847                 CLNT_CONTROL(client, CLSET_VERS, (char *)&vers);
848                 clnt_st = CLNT_CALL(client, RPCBPROC_GETADDR,
849                     (xdrproc_t)xdr_rpcb, (char *)&parms,
850                     (xdrproc_t)xdr_wrapstring, (char *)&ua, *tp);
851                 /* Sets error structure members in client handle */
852                 switch (clnt_st) {
853                 case RPC_SUCCESS: /* Call succeeded */
854                         if (ua != NULL) {
855                                 if (ua[0] != '\0') {
856                                         address = uaddr2taddr(nconf, ua);
857                                 }
858                                 xdr_free((xdrproc_t)xdr_wrapstring,
859                                     (char *)&ua);
984                                 (xdrproc_t)xdr_wrapstring,
985                                 (char *)&ua, *tp);
986                 if (clnt_st == RPC_SUCCESS) {
987                         if ((ua == NULL) || (ua[0] == NULL)) {
988                                 if (ua != NULL)
989                                         xdr_free(xdr_wrapstring, (char *)&ua);

861                                 if (address != NULL) {
862                                         goto done;
863                                 }
864                                 /* We don't know about your universal addr */
865                                 /* cf_error is still zeroed */
```



```
991                                 /* address unknown */
866                                 rpc_createerr.cf_stat = RPC_PROGNOTREGISTERED;
867                                 goto error;
868                         }
869 #ifndef PORTMAP
870                         clnt_geterr(client, &rpc_createerr.cf_error);
871                         rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
872                         goto error;
995                         address = uaddr2taddr(nconf, ua);
996 #ifdef ND_DEBUG
997                         fprintf(stderr, "\tRemote address is [%s]\n", ua);
998                         if (!address)
999                                 fprintf(stderr,
1000                                         "\tCouldn't resolve remote address!\n");
873 #endif
874                         /* Try the next version */
875                         break;
876                 case RPC_PROGVERSMISMATCH: /* RPC protocol mismatch */
877                         clnt_geterr(client, &rpc_createerr.cf_error);
878 #ifdef PORTMAP
879                         if (rpc_createerr.cf_error.re_vers.low > vers) {
880                                 rpc_createerr.cf_stat = clnt_st;
881                                 goto error;  /* a new version, can't handle */
882                         }
883 #else
884                         rpc_createerr.cf_stat = clnt_st;
885                         goto error;
886 #endif
887                         /* Try the next version */
888                         break;
889 #ifdef PORTMAP
890                 case RPC_PROCUNAVAIL: /* Procedure unavailable */
891                 case RPC_PROGUNAVAIL: /* Program not available */
892                 case RPC_TIMEDOUT: /* Call timed out */
893                         /* Try the next version */
894                         break;
895 #endif
896                 default:
897                         clnt_geterr(client, &rpc_createerr.cf_error);
898                         rpc_createerr.cf_stat = RPC_PMAPFAILURE;
899                         goto error;
900                         break;
901                 }
902         } /* End of version 3 */
903 #ifndef PORTMAP
904         /* cf_error members set by creation failure */
905         rpc_createerr.cf_stat = RPC_PROGNOTREGISTERED;
906 #endif
907         /*
908          * Try version 2
909          */
1002                        xdr_free((xdrproc_t)xdr_wrapstring, (char *)&ua);

911 #ifdef PORTMAP
912         /* Try version 2 for TCP or UDP */
913         if (strcmp(nconf->nc_protofmly, NC_INET) == 0) {
914                 ushort_t port = 0;
915                 struct netbuf remote;
916                 uint_t pmapvers = 2;
917                 struct pmap pmapparms;

919                 /*
920                  * Try UDP only - there are some portmappers out
921                  * there that use UDP only.
922                  */
923                 if (strcmp(nconf->nc_proto, NC_TCP) == 0) {
```

```
924                         struct netconfig *newnconf;
926                         if (client != NULL) {
927                                 CLNT_DESTROY(client);
928                                 client = NULL;
929                                 free(parms.r_addr);
930                                 parms.r_addr = NULL;
931                         }
932                         if ((handle = __rpc_setconf("udp")) == NULL) {
933                                 /* cf_error is still zeroed */
934                                 rpc_createerr.cf_stat = RPC_UNKNOWNPROTO;
1004                        if (!address) {
1005                                /* We don't know about your universal address */
1006                                rpc_createerr.cf_stat = RPC_N2AXLATEFAILURE;
935                                 goto error;
936                         }
1009                        goto done;
1010                }
1011                if (clnt_st == RPC_PROGVERSMISMATCH) {
1012                        struct rpc_err rpcerr;
938                         /*
939                          * The following to reinforce that you can
940                          * only request for remote address through
941                          * the same transport you are requesting.
942                          * ie. requesting unversial address
943                          * of IPv4 has to be carried through IPv4.
944                          * Can't use IPv6 to send out the request.
945                          * The mergeaddr in rpcbind can't handle
946                          * this.
947                          */
948                         for (;;) {
949                                 if ((newnconf = __rpc_getconf(handle))
950                                     == NULL) {
951                                         __rpc_endconf(handle);
952                                         /* cf_error is still zeroed */
953                                         rpc_createerr.cf_stat =
954                                             RPC_UNKNOWNPROTO;
1014                        clnt_geterr(client, &rpcerr);
1015                        if (rpcerr.re_vers.low > RPCBVERS4)
1016                                goto error;  /* a new version, can't handle */
1017                } else if (clnt_st != RPC_PROGUNAVAIL) {
1018                        /* Cant handle this error */
955                                         goto error;
956                                 }
957                                 /*
958                                  * here check the protocol family to
959                                  * be consistent with the request one
960                                  */
961                                 if (strcmp(newnconf->nc_protofmly,
962                                     nconf->nc_protofmly) == 0)
963                                         break;
964                         }
966                         client = _getclnthandle_timed(host, newnconf,
967                             &parms.r_addr, tp);
968                         /* Sets cf_error members on failure */
969                         __rpc_endconf(handle);
970                         tmp_client = TRUE;
971                 }
972                 if (client == NULL) {
973                         /* cf_error members set by creation failure */
1023        if ((address == NULL) || (address->len == 0)) {
974                         rpc_createerr.cf_stat = RPC_PROGNOTREGISTERED;
975                         tmp_client = FALSE;
976                         goto error;
```



```
977                 }
979                 /*
980                  * Set version and retry timeout.
981                  */
982                 CLNT_CONTROL(client, CLSET_RETRY_TIMEOUT, (char *)&rpcbrmttime);
983                 CLNT_CONTROL(client, CLSET_VERS, (char *)&pmapvers);
985                 pmapparms.pm_prog = program;
986                 pmapparms.pm_vers = version;
987                 pmapparms.pm_prot = (strcmp(nconf->nc_proto, NC_TCP) != 0) ?
988                     IPPROTO_UDP : IPPROTO_TCP;
989                 pmapparms.pm_port = 0;  /* not needed */
990                 clnt_st = CLNT_CALL(client, PMAPPROC_GETPORT,
991                     (xdrproc_t)xdr_pmap, (caddr_t)&pmapparms,
992                     (xdrproc_t)xdr_u_short, (caddr_t)&port, *tp);
993                 /* Sets error structure members in client handle */
994                 if (clnt_st != RPC_SUCCESS) {
995                         clnt_geterr(client, &rpc_createerr.cf_error);
996                         rpc_createerr.cf_stat = RPC_RPCBFAILURE;
997                         goto error;
998                 } else if (port == 0) {
999                         /* cf_error is still zeroed */
1000                        rpc_createerr.cf_stat = RPC_PROGNOTREGISTERED;
1001                        goto error;
1002                }
1003                port = htons(port);
1004                CLNT_CONTROL(client, CLGET_SVC_ADDR, (char *)&remote);
1005                if (((address = malloc(sizeof (struct netbuf))) == NULL) ||
1006                    ((address->buf = malloc(remote.len)) == NULL)) {
1007                        /* cf_error is still zeroed */
1008                        rpc_createerr.cf_error.re_errno = errno;
1009                        rpc_createerr.cf_stat = RPC_SYSTEMERROR;
1010                        free(address);
1011                        address = NULL;
1012                        goto error;
1013                }
1014                (void) memcpy(address->buf, remote.buf, remote.len);
1015                (void) memcpy(&address->buf[sizeof (short)], &port,
1016                    sizeof (short));
1017                address->len = address->maxlen = remote.len;
1018                goto done;
1019        } else {
1020                /* Not NC_INET */
1021                if (client != NULL && clnt_st != RPC_SUCCESS) {
1022                        clnt_geterr(client, &rpc_createerr.cf_error);
1023                        rpc_createerr.cf_stat = clnt_st;
1024                } else {
1025                        /* No client handle */
1026                        rpc_createerr.cf_stat = RPC_SYSTEMERROR;
1027                }
1028        }
1029 #endif
1031 error:
1032        /* Return NULL address and NULL client */
1033        address = NULL;
1034        if (client != NULL) {
1029        if (client) {
1035                CLNT_DESTROY(client);
1036                client = NULL;
1037        }
1039 done:
1040        /* Return an address and optional client */
1041        if (client != NULL && tmp_client) {
```

```
1042                    /* This client is the temporary one */
1034            if (nconf->nc_semantics != NC_TPI_CLTS) {
1035                    /* This client is the connectionless one */
1036                    if (client) {
1043                    CLNT_DESTROY(client);
1044                    client = NULL;
1045            }
1046            if (clpp != NULL) {
1040            }
1041            if (clpp) {
1047                    *clpp = client;
1048            } else if (client != NULL) {
1043            } else if (client) {
1049                    CLNT_DESTROY(client);
1050            }
1046            if (parms.r_addr)
1051            free(parms.r_addr);
1052            return (address);
1053 }
```

_____***unchanged_portion_omitted_***