Bip - Bug #262

using ircnet bip crashes if a channel has two nicks different only by one "~"

2011-11-13 16:30 - Pierre-Louis Bonicoli

Status:	In Progress	**Start date:**	2011-11-13
Priority:	Normal	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	50%
Category:		**Estimated time:**	0.00 hour
Target version:			
Patch Available:	Yes	**Branch:**	
Found in Versions:		**Security:**	Yes
Confirmed:	Yes	**Help Needed:**	No

Description

nitram reported:

```
as soon as i join a channel that has the nicks "~mc" and "mc" on ircnet bip crashes with "11-11-20
11 15:55:44 FATAL: Element with key mc already in hash b9495ce0
```

I found two problems:

First, in irc_353 function (source:src/irc.c@a46b8bd2#L1362) we discard '~' character when storing operator/voice mask foreach nickname. For example if the irc server send
'ircnet.optilian.net' ':ircnet.optilian.net 353 pilou = #plopplopplop :pilou ~lolll219 lolll219 ' (user pilou joining ircnet.optilian.net where tho users ~lolll219 lolll219 are here)
we store operator/voice mask of lolll219 twice (once for ~lolll219 and another for lolll219).

This lead to many errors:

- if either lolll219 or ~lolll219 have a not empty operator/voice mask, then problem reported by nitram appears: the second hash_insert fails.
- when ~lolll219 or lolll219 send irc part command, irc_part function (source:src/irc.c@a46b8bd2#L1498) encounters problem. If ~lolll219 quit then his operator/voice mask can not be found (it was not stored) and then irc_part return ERR_PROTOCOL:

```
13-11-2011 14:38:22 ERROR: [ircnet] Error in protocol, closing...
13-11-2011 14:38:22 ERROR: [ircnet] reconnecting in 0 seconds
```

- If lolll219 quit then an assertion fails, indeed the lolll219 key is present twice in the operator/voice mask hash:

```
13-11-2011 14:37:29 FATAL: 80b3288 appears twice in list
```

Second problem: it should not be possible to store two identical key in one hash. list_remove_if_exists function (source:src/util.c@a46b8bd2#L370) - called by irc_part - verify this assertion and the assertion fails.

Currently insertion of two identical keys occurs because instead of checking if the hash contains already an identical key, we check if the value corresponding to this key is NULL or not (source:src/util.c@a46b8bd2#L566):

```
void hash_insert(hash_t *hash, const char *key, void *ptr)
[...]
    if (hash_get(hash, key))
```

```
        fatal("Element with key %s already in hash %x\n", key, hash);
```

So it's possible to store many identical key associated to 0/NULL value.

And the associated value for the key in operator/voice mask hash can be 0/NULL:

```
long int ovmask = 0;
[...]
hash_insert(&channel->ovmasks, nick, (void *)ovmask);
```

History

#1 - 2011-11-13 16:32 - Pierre-Louis Bonicoli

- File 0001-hash_insert-check-if-key-isn-t-already-here-before.patch added

- File 0001-ircnet-servers-allow-in-nickname.patch added

- Status changed from New to In Progress

- % Done changed from 0 to 50

- Patch Available changed from No to Yes

- Confirmed changed from No to Yes

- Security changed from No to Yes

Patchs need to be reviewed by nohar :)

#2 - 2011-11-16 02:11 - Pierre-Louis Bonicoli

hash_includes is sufficient, hash_has_key is redundant.

I do some tests with unrealirc, thanks to Nathan Brink (aka binki) !

- logs for names / join:

```
16-11-2011 01:42:15 DEBUG: ":irc1.unrealircd.org 353 Pilou = #plopplopplop2 :~coincoinlol2 ~binki &Pilou @
coincoinlol "
```

- logs for part:

```
16-11-2011 01:43:04 DEBUG: ":coincoinlol2!~lilou@Clk-8B8C976E.fbx.proxad.net PART #plopplopplop2"
```

ircnet allows "~" at the beginning of nicknames. Then "~" appears in /part and /names.

Therefore patch need modifications: when connecting to an irc server he send something like

```
02:07:50    ircnet  -- | Welcome to the Internet Relay Network pilou!~pilou@did75-2-81-57-106-132.fbx.proxad.n
et
02:07:50    ircnet  -- | Your host is ircnet.optilian.net, running version 2.11.2p2
02:07:50    ircnet  -- | This server was created Sun Nov 21 2010 at 22:28:21 CET
02:07:50    ircnet  -- | ircnet.optilian.net 2.11.2p2 aoOirw abeiIklmnoOpqrRstv
02:07:50    ircnet  -- | RFC2812 PREFIX=(ov)@+ CHANTYPES=#&!+ MODES=3 CHANLIMIT=#&!+:21 NICKLEN=15 TOPICLEN=25
5 KICKLEN=255 MAXLIST=beIR:64 CHANNELLEN=50 IDCHAN=!:5
                      | CHANMODES=beIR,k,l,imnpstaqr :are supported by this server
02:07:50    ircnet  -- | PENALTY FNC EXCEPTS=e INVEX=I CASEMAPPING=ascii NETWORK=IRCnet :are supported by this
 server
```

PREFIX variable must be used in order to fix the bug. PREFIX for unrealircd is PREFIX=(qaohv)~&%+@

#3 - 2013-10-19 12:39 - Marc Dequènes

- Target version deleted (0.8.9)

- Help Needed set to No

Files

0001-hash_insert-check-if-key-isn-t-already-here-before.patch	1.63 KB	2011-11-13	Pierre-Louis Bonicoli
0001-ircnet-servers-allow-in-nickname.patch	701 Bytes	2011-11-13	Pierre-Louis Bonicoli