Quassel IRC - Bug #1473

Quassel Client does not remember the channel encryption key set using /setkey

02/06/2018 12:48 AM - gry

Status:	Resolved	**Start date:**	02/06/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
Version:	0.12.4	**OS:**	Any

Description

Steps:

1. /setkey #chan foo
2. close Quassel Client and re-open it

Expected result:

1. the encryption key is remembered

Actual result:

1. the encryption key is reset, plain text messages are sent

Associated revisions

Revision c382e0c1 - 05/24/2018 12:33 AM - mamarley

Persist Blowfish keys in the database

Add a new text field called "cipher" and store the hex-encoded cipher key there whenever a new key is set or exchanged. Also, when each network is initialized, load the ciphers out of the database and initialize the in-memory hashmap. Then, the existing behavior of each CoreIrcNetwork automatically using these keys upon construction occurs.

Additionally, this makes PM buffer ciphers persistent both across destruction/construction and across core restarts.

Note that the existing "key" field in the database is confusingly named. It does not contain any sort of cryptographic key but instead holds channel passwords.

Closes #1473

Closes GH-332.

History

#1 - 05/24/2018 12:33 AM - mamarley

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset quassel|c382e0c11f80fb37307ecc42c487aa433c97ad8c.