MSG\_DEBUG / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_GROUP / KeyExchangeInitMessage, DisconnectMessage MSG KEX DH GEX OLD REQUEST / KeyExchangeInitMessage, DisconnectMessage MSG\_KEX\_DH\_GEX\_REPLY / KeyExchangeInitMessage,UnimplementedMessage MSG\_KEXDH\_INIT / KeyExchangeInitMessage, DisconnectMessage MSG\_KEXDH\_REPLY / KeyExchangeInitMessage, DisconnectMessage MSG\_DISCONNECT / KeyExchangeInitMessage MSG\_KEX\_ECDH\_INIT / KeyExchangeInitMessage,DisconnectMessage MSG\_KEX\_ECDH\_REPLY / KeyExchangeInitMessage, DisconnectMessage MSG\_EXT\_INFO / KevExchangeInitMessage.DisconnectMessage MSG\_KEX\_HBR\_INIT / KeyExchangeInitMessage,DisconnectMessage MSG\_KEX\_HBR\_REPLY / KeyExchangeInitMessage,DisconnectMessage MSG\_IGNORE / KevExchangeInitMessage MSG\_NEWCOMPRESS / KeyExchangeInitMessage,UnimplementedMessage MSG\_PING\_OPENSSH / KeyExchangeInitMessage,UnimplementedMessage MSG\_PONG\_OPENSSH / KeyExchangeInitMessage,UnimplementedMessage MSG\_KEX\_RSA\_DONE / KeyExchangeInitMessage,UnimplementedMessage MSG KEX RSA PUBKEY / KeyExchangeInitMessage.DisconnectMessage MSG\_KEX\_RSA\_SECRET / KeyExchangeInitMessage, DisconnectMessage MSG\_SERVICE\_ACCEPT / KeyExchangeInitMessage,DisconnectMessage MSG\_SERVICE\_REQUEST\_CONNECTION / KeyExchangeInitMessage,DisconnectMessage MSG\_UNIMPLEMENTED / KeyExchangeInitMessage MSG\_VERSION\_EXCHANGE / KeyExchangeInitMessage,UnimplementedMessage MSG\_USERAUTH\_BANNER / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_FAILURE / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_INFO\_REQUEST / KeyExchangeInitMessage, DisconnectMessage MSG\_USERAUTH\_INFO\_RESPONSE / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_PASSWD\_CHANGEREQ / KeyExchangeInitMessage, DisconnectMessage MSG\_USERAUTH\_PK\_OK / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_REQUEST\_HOSTBASED / KeyExchangeInitMessage, DisconnectMessage MSG\_USERAUTH\_REQUEST\_KEYBOARD\_INTERACTIVE / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_REQUEST\_NONE / KeyExchangeInitMessage, DisconnectMessage MSG\_USERAUTH\_REQUEST\_PASSWORD / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_REQUEST\_PUBLICKEY\_HOSTBOUND\_OPENSSH / KeyExchangeInitMessage,DisconnectMessage MSG\_USERAUTH\_REQUEST\_PUBLICKEY / KeyExchangeInitMessage, DisconnectMessage MSG\_USERAUTH\_REQUEST\_UNKNOWN / KeyExchangeInitMessage, DisconnectMessage MSG USERAUTH SUCCESS / KevExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_CLOSE / KeyExchangeInitivlessage, DisconnectMessage MSG\_CHANNEL\_DATA / KcyExchangeInitMessage, DisconnectMessage MSG CHANNEL EOF / KeyExchangeInitMessage, DisconnectMessage MSG CHANNEL\_EXTENDED\_DATA / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_FAILURE / KevEvchangeInitMessage\_DisconnectMessage MSG CHANNEL OPEN CONFIRMATION / KeyExchangeInitMessage, DisconnectMessage MSG CHANNEL\_OPEN\_DIRECT\_STREAMLOCAL\_OPENSSH / KeyExchangeInitMessage, DisconnectMessage Protocol Completed MSG\_CHANNEL\_OPEN\_DIRECT\_TCPIP / KeyExchangeInitMessage.DisconnectMessage MSG\_KEX\_DH\_GEX\_INIT / KeyExchangeInitMessage, UnimplementedMessage, UnimplementedMessage MSG CHANNEL OPEN FAILURE / KeyExchangeInitMessage, DisconnectMessage SocketState: [UP, CLOSED] MSG\_CHANNEL\_OPEN\_FORWARDED\_STREAMLOCAL\_OPENSSH / KeyExchangeInitMessage\_DisconnectMessage MSG\_CHANNEL\_OPEN\_FORWARDED\_ICPIP / KeyExchangeInitMessage,DisconnectMessage
MSG\_CHANNEL\_OPEN\_SESSION / KcyExchangeInitMessage,DisconnectMessage
MSG\_CHANNEL\_OPEN\_TUN\_OPENSSH / KcyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_OPEN\_UNKNOWN / KeyExchangeInitMessage, DisconnectMessage
MSG\_CHANNEL\_OPEN\_X11 / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_AUTH\_AGENT\_OPENSSH / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_REQUEST\_BREAK / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_ENV / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_EOW\_OPENSSH / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_REQUEST\_EXEC / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_EXIT\_SIGNAL / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_REQUEST\_EXIT\_STATUS / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_REQUEST\_PTY\_REQ / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_SHELL / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_SIGNAL / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_SUBSYSTEM / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_UNKNOWN / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_REQUEST\_WINDOW\_CHANGE / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_X11\_REQ / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_REQUEST\_XON\_XOFF / KeyExchangeInitMessage, DisconnectMessage MSG\_CHANNEL\_SUCCESS / KeyExchangeInitMessage,DisconnectMessage MSG\_CHANNEL\_WINDOW\_ADJUST / KeyExchangeInitMessage,DisconnectMessage MSG\_GLOBAL\_REQUEST\_CANCEL\_STREAMLOCAL\_FORWARD\_OPENSSH / KeyExchangeInitMessage, DisconnectMessage MSG\_GLOBAL\_REQUEST\_CANCEL\_TCPIP\_FORWARD / KeyExchangeInitMessage, DisconnectMessage MSG\_REQUEST\_FAILURE / KeyExchangeInitMessage, DisconnectMessage MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_OPENSSH / KeyExchangeInitMessage,DisconnectMessage MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_PROVE\_OPENSSH / KeyExchangeInitMessage, DisconnectMessage MSG GLOBAL REQUEST NO MORE SESSIONS OPENSSH / KeyExchangeInitMessage, DisconnectMessage MSG\_GLOBAL\_REQUEST\_STREAMLOCAL\_FORWARD\_OPENSSH / KeyExchangeInitMessage, DisconnectMessage MSG\_REQUEST\_SUCCESS / KeyExchangeInitMessage, DisconnectMessage MSG\_GLOBAL\_REQUEST\_TCPIP\_FORWARD / KeyExchangeInitMessage, DisconnectMessage MSG\_GLOBAL\_REQUEST\_UNKNOWN / KeyExchangeInitMessage, DisconnectMessage MSG\_UNKNOWN\_ID\_RESERVED\_0 / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_TRANSPORT\_GENERIC / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_ALGORITHM\_NEGOTIATION / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_KEY\_EXCHANGE\_SPECIFIC / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_USERAUTH\_GENERIC / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_USERAUTH\_SPECIFIC / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_CONNECTION\_GENERIC / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_CHANNEL\_RELATED / KeyExchangeInitMessage,UnimplementedMessage MSG\_UNKNOWN\_ID\_RESERVED\_CLIENT / KeyExchangeInitMessage,UnimplementedMessage MSG UNKNOWN ID RESERVED PRIVATE / KeyExchangeInitMessage,UnimplementedMessage Server/Client: libssh 0.11.1 Protocol Stage: TRANSPORT KEX Algorithm: diffie-hellman-group-exchange-sha256 Strict KEX enabled: true

Messages used during testing: MSG\_DEBUG MSG\_KEX\_DH\_GEX\_GROUP MSG\_KEX\_DH\_GEX\_INIT MSG\_KEX\_DH\_GEX\_OLD\_REQUEST MSG\_KEX\_DH\_GEX\_REPLY MSG\_KEX\_DH\_GEX\_REQUEST MSG\_KEXDH\_INIT MSG\_KEXDH\_REPLY MSG\_DISCONNECT MSG\_KEX\_ECDH\_INIT MSG\_KEX\_ECDH\_REPLY MSG\_EXT\_INFO MSG\_KEX\_HBR\_INIT MSG\_KEX\_HBR\_REPLY MSG\_IGNORE MSG\_KEXINIT MSG\_NEWCOMPRESS MSG\_NEWKEYS MSG\_PING\_OPENSSH MSG\_PONG\_OPENSSH MSG\_KEX\_RSA\_DONE MSG\_KEX\_RSA\_PUBKEY MSG\_KEX\_RSA\_SECRET MSG\_SERVICE\_ACCEPT MSG\_SERVICE\_REQUEST\_USERAUTH MSG\_SERVICE\_REQUEST\_CONNECTION MSG\_UNIMPLEMENTED MSG\_VERSION\_EXCHANGE MSG\_USERAUTH\_BANNER MSG\_USERAUTH\_FAILURE MSG\_USERAUTH\_INFO\_REQUEST MSG\_USERAUTH\_INFO\_RESPONSE MSG\_USERAUTH\_PASSWD\_CHANGEREQ MSG\_USERAUTH\_PK\_OK MSG\_USERAUTH\_REQUEST\_HOSTBASED MSG\_USERAUTH\_REQUEST\_KEYBOARD\_INTERACTIVE MSG\_USERAUTH\_REQUEST\_NONE MSG\_USERAUTH\_REQUEST\_PASSWORD MSG\_USERAUTH\_REQUEST\_PUBLICKEY\_HOSTBOUND\_OPENSSH MSG\_USERAUTH\_REQUEST\_PUBLICKEY MSG\_USERAUTH\_REQUEST\_UNKNOWN MSG\_USERAUTH\_SUCCESS MSG\_CHANNEL\_CLOSE MSG\_CHANNEL\_DATA MSG\_CHANNEL\_EOF MSG\_CHANNEL\_EXTENDED\_DATA MSG\_CHANNEL\_FAILURE MSG\_CHANNEL\_OPEN\_CONFIRMATION MSG\_CHANNEL\_OPEN\_DIRECT\_STREAMLOCAL\_OPENSSH MSG\_CHANNEL\_OPEN\_DIRECT\_TCPIP MSG\_CHANNEL\_OPEN\_FAILURE MSG\_CHANNEL\_OPEN\_FORWARDED\_TCPIP MSG\_CHANNEL\_OPEN\_SESSION

MSG\_CHANNEL\_OPEN\_FORWARDED\_STREAMLOCAL\_OPENSSH MSG\_CHANNEL\_OPEN\_TUN\_OPENSSH MSG\_CHANNEL\_OPEN\_UNKNOWN MSG\_CHANNEL\_OPEN\_X11 MSG\_CHANNEL\_REQUEST\_AUTH\_AGENT\_OPENSSH

> MSG\_CHANNEL\_REQUEST\_BREAK MSG\_CHANNEL\_REQUEST\_ENV MSG\_CHANNEL\_REQUEST\_EOW\_OPENSSH MSG\_CHANNEL\_REQUEST\_EXEC MSG\_CHANNEL\_REQUEST\_EXIT\_SIGNAL MSG\_CHANNEL\_REQUEST\_EXIT\_STATUS MSG\_CHANNEL\_REQUEST\_PTY\_REQ MSG\_CHANNEL\_REQUEST\_SHELL MSG\_CHANNEL\_REQUEST\_SIGNAL MSG\_CHANNEL\_REQUEST\_SUBSYSTEM MSG\_CHANNEL\_REQUEST\_UNKNOWN MSG\_CHANNEL\_REQUEST\_WINDOW\_CHANGE MSG\_CHANNEL\_REQUEST\_X11\_REQ

MSG\_CHANNEL\_SUCCESS MSG\_CHANNEL\_WINDOW\_ADJUST MSG\_GLOBAL\_REQUEST\_CANCEL\_STREAMLOCAL\_FORWARD\_OPENSSH MSG\_GLOBAL\_REQUEST\_CANCEL\_TCPIP\_FORWARD MSG\_REQUEST\_FAILURE

MSG\_CHANNEL\_REQUEST\_XON\_XOFF

MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_OPENSSH MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_PROVE\_OPENSSH MSG\_GLOBAL\_REQUEST\_NO\_MORE\_SESSIONS\_OPENSSH MSG\_GLOBAL\_REQUEST\_STREAMLOCAL\_FORWARD\_OPENSSH MSG\_REQUEST\_SUCCESS

> MSG\_GLOBAL\_REQUEST\_TCPIP\_FORWARD MSG\_GLOBAL\_REQUEST\_UNKNOWN MSG\_UNKNOWN\_ID\_RESERVED\_0 MSG\_UNKNOWN\_ID\_TRANSPORT\_GENERIC MSG\_UNKNOWN\_ID\_ALGORITHM\_NEGOTIATION MSG\_UNKNOWN\_ID\_KEY\_EXCHANGE\_SPECIFIC MSG\_UNKNOWN\_ID\_USERAUTH\_GENERIC MSG\_UNKNOWN\_ID\_USERAUTH\_SPECIFIC MSG\_UNKNOWN\_ID\_CONNECTION\_GENERIC MSG\_UNKNOWN\_ID\_CHANNEL\_RELATED MSG UNKNOWN ID RESERVED CLIENT MSG\_UNKNOWN\_ID\_RESERVED\_PRIVATE