MSG\_DEBUG / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_GROUP / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_INIT / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_OLD\_REQUEST / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_REPLY / KeyExchangeInitMessage MSG\_KEX\_DH\_GEX\_REQUEST / KeyExchangeInitMessage MSG\_KEXDH\_REPLY / KeyExchangeInitMessage MSG\_DISCONNECT / KeyExchangeInitMessage MSG\_KEX\_ECDH\_INIT / KeyExchangeInitMessage MSG\_KEX\_ECDH\_REPLY / KeyExchangeInitMessage MSG EXT INFO / KevExchangeInitMessage MSG KEX HBR INIT / KeyExchangeInitMessage MSG\_KEX\_HBR\_REPLY / KeyExchangeInitMessage MSG IGNORE / KeyExchangeInitMessage MSG\_NEWCOMPRESS / KeyExchangeInitMessage MSG\_PING\_OPENSSH / KeyExchangeInitMessage MSG\_PONG\_OPENSSH / KeyExchangeInitMessage MSG\_KEX\_RSA\_DONE / KeyExchangeInitMessage MSG KEX RSA PUBKEY / KeyExchangeInitMessage MSG\_KEX\_RSA\_SECRET / KeyExchangeInitMessage MSG\_SERVICE\_ACCEPT / KeyExchangeInitMessage MSG\_SERVICE\_REQUEST\_CONNECTION / KeyExchangeInitMessage MSG\_UNIMPLEMENTED / KeyExchangeInitMessage MSG\_USERAUTH\_BANNER / KeyExchangeInitMessage MSG\_USERAUTH\_FAILURE / KeyExchangeInitMessage MSG\_USERAUTH\_INFO\_REQUEST / KeyExchangeInitMessage MSG USERAUTH INFO RESPONSE / KeyExchangeInitMessage MSG\_USERAUTH\_PASSWD\_CHANGEREQ / KeyExchangeInitMessage MSG\_USERAUTH\_PK\_OK / KeyExchangeInitMessage MSG\_USERAUTH\_REQUEST\_HOSTBASED / KeyExchangeInitMessage MSG\_USERAUTH\_REQUEST\_KEYBOARD\_INTERACTIVE / KeyExchangeInitMessage MSG\_USERAUTH\_REQUEST\_NONE / KeyExchangeInitMessage MSG\_USERAUTH\_REQUEST\_PASSWORD / KeyExchangeInitMessage MSG\_USERAUTH\_REQUEST\_PUBLICKEY\_HOSTBOUND\_OPENSSH / KeyExchangeInitMessage MSG USERAUTH REOUEST PUBLICKEY / KevExchangeInitMessage MSG\_USERAUTH\_REQUEST\_UNKNOWN / KeyExchangeInitMessage MSG\_USERAUTH\_SUCCESS / KeyExchangeInitMessage MSG\_CHANNEL\_CLOSE / KevFxchangeInitMessag MSG-CHANNEL DATA / KeyExchangeInitMessage MSG\_CHANNEL\_EOF / KeyExchangeInitMessage MSG\_CHANNEL EXTENDED DATA / KeyExchangeInitMessage MSG\_CHANNEL\_FAILURE / KeyExchangeInitMessage MSG\_CHANNEL\_OPEN\_CONFIRMATION / KeyExchangeInitMessage Protocol Completed MSG\_CHANNEL\_OPEN\_DIRECT\_STREAMLOCAL\_OPENSSH / KeyExchangeInitMessage MSG\_CHANNEL\_OPEN\_DIRECT\_TCPIP / KeyExchangeInitMessage MSG\_KEXDH\_INIT / KevExchangeInitMessageMSG\_KEXINIT / KevExchangeInitMessageMSG\_NEWKEYS / KevExchangeInitMessage |SocketState: [UP, CLOSED] MSG CHANNEL OPEN FAILURE / KeyExchangeInitMessage MSG CHANNEL OPEN FORWARDED STREAMLOCAL OPENSSH / KeyExchangeInitMessage MSG CHANNEL OPEN FORWARDED TCPIP / KeyExchangeInitMessage MSG CHANNEL\_OPEN\_SESSION / KeyExchangeInitMessage MSG CHANNEL OPEN TUN OPENSSH / KeyExchangeInitMessage MSG CHANNEL OPEN UNKNOWN / KeyExchangeInitMessage MSG CHANNEL OPEN X11 / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_AUTH\_AGENT\_OPENSSH / KcyExchangeInitMessage MSG CHANNEL REQUEST BREAK / KeyExchangeInitMessage MSG CHANNEL REOUEST ENV / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_EOW\_OPENSSH / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_EXEC / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_EXIT\_SIGNAL / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_EXIT\_STATUS / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_PTY\_REQ / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_SHELL / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_SIGNAL / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_SUBSYSTEM / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_UNKNOWN / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_WINDOW\_CHANGE / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_X11\_REQ / KeyExchangeInitMessage MSG\_CHANNEL\_REQUEST\_XON\_XOFF / KeyExchangeInitMessage MSG\_CHANNEL\_SUCCESS / KeyExchangeInitMessage MSG\_CHANNEL\_WINDOW\_ADJUST / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_CANCEL\_STREAMLOCAL\_FORWARD\_OPENSSH / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_CANCEL\_TCPIP\_FORWARD / KeyExchangeInitMessage MSG\_REQUEST\_FAILURE / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_OPENSSH / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_HOSTKEYS\_PROVE\_OPENSSH / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_NO\_MORE\_SESSIONS\_OPENSSH / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_STREAMLOCAL\_FORWARD\_OPENSSH / KeyExchangeInitMessage MSG\_REQUEST\_SUCCESS / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_TCPIP\_FORWARD / KeyExchangeInitMessage MSG\_GLOBAL\_REQUEST\_UNKNOWN / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_RESERVED\_0 / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_TRANSPORT\_GENERIC / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_ALGORITHM\_NEGOTIATION / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_KEY\_EXCHANGE\_SPECIFIC / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_USERAUTH\_GENERIC / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_USERAUTH\_SPECIFIC / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_CONNECTION\_GENERIC / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_CHANNEL\_RELATED / KeyExchangeInitMessage MSG\_UNKNOWN\_ID\_RESERVED\_CLIENT / KeyExchangeInitMessage MSG UNKNOWN ID RESERVED PRIVATE / KevExchangeInitMessage Server/Client: x/crypto/ssh 0.37.0 Protocol Stage: TRANSPORT KEX Algorithm: diffie-hellman-group14-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\_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\_STREAMLOCAL\_OPENSSH MSG\_CHANNEL\_OPEN\_FORWARDED\_TCPIP MSG CHANNEL\_OPEN\_SESSION 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\_REQUEST\_XON\_XOFF MSG\_CHANNEL\_SUCCESS MSG\_CHANNEL\_WINDOW\_ADJUST MSG\_GLOBAL\_REQUEST\_CANCEL\_STREAMLOCAL\_FORWARD\_OPENSSH MSG\_GLOBAL\_REQUEST\_CANCEL\_TCPIP\_FORWARD MSG\_REQUEST\_FAILURE 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