



Server/Client: LANCOM LCOS 10.90.0126 Rel  
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\_KEXDH\_INIT
  - MSG\_KEXDH\_REPLY
  - MSG\_DISCONNECT
  - MSG\_KEXECDH\_INIT
  - MSG\_KEXECDH\_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\_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\_GLOBAL\_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\_FAILURE
  - 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\_SPECIFIC
  - MSG\_UNKNOWN\_ID\_CONNECTION\_GENERIC
  - MSG\_UNKNOWN\_ID\_CHANNEL\_RELATED
  - MSG\_UNKNOWN\_ID\_RESERVED\_CLIENT
  - MSG\_UNKNOWN\_ID\_RESERVED\_PRIVATE