QUIC10GS-IP Demo Instruction

QUIC10GS-IP Demo Instruction

Rev1.00 12-Mar-2025

This document provides detailed instructions to demonstrate the use of the QUIC Server 10Gbps IP core (QUIC10GS-IP) on our reference design, referred to as the “QUIC10GS-IP Reference Design”, using the KCU116 development board. The QUIC10GS-IP is used as a medium to transfer data within a secure connection following the QUIC transport protocol version 1 standard (RFC9000). This process involves handling the TLS 1.3 handshake and dealing with data encryption and decryption.

The reference design uses the QUIC10GS-IP and manages the application layer of the IP. It is tailored to test the IP functionality, to help users understand how to use the IP, and to offer flexibility for users in case they need to modify the design. The main application demonstrated in this reference design is a unique application protocol designed by an organization to use with their application.

This instruction will explain step-by-step how users can utilize the QUIC10GS-IP through our reference design for uploading and downloading data. MsQuic is employed as a client to show the transfer performance using the unique application protocol.

Following our document guidelines, this document will describe how to set up the environment for the test, provide more details about the reference example (MsQuic), and instruct and show the results of the test, respectively.

1 Environment Setup

To run the QUIC10GS-IP demo, please prepare following test environment.

1) FPGA development boards (KCU116 development board).
2) Test PC with 10 Gigabit Ethernet or connecting with 10 Gigabit Ethernet card.
3) 10 Gb Ethernet cable:
    a) 10 Gb SFP+ Passive Direct Attach Cable (DAC) which has 1-m or less length
    b) 10 Gb SFP+ Active Optical Cable (AOC)
    c) 2x10 Gb SFP+ transceiver (10G BASE-R) with optical cable (LC to LC, Multimode)
4) Micro USB cable for JTAG connection connecting between FPGA board and Test PC.
5) Micro USB cable for UART connection connecting between FPGA board and Test PC.
6) Vivado tool for programming FPGA installed on Test PC.
7) Serial console software such as TeraTerm installed on PC. The setting on the console is Baudrate=115200, Data=8-bit, Non-parity and Stop=1.
8) Demo configuration file (To download this file, please visit our web site at www.design-gateway.com).

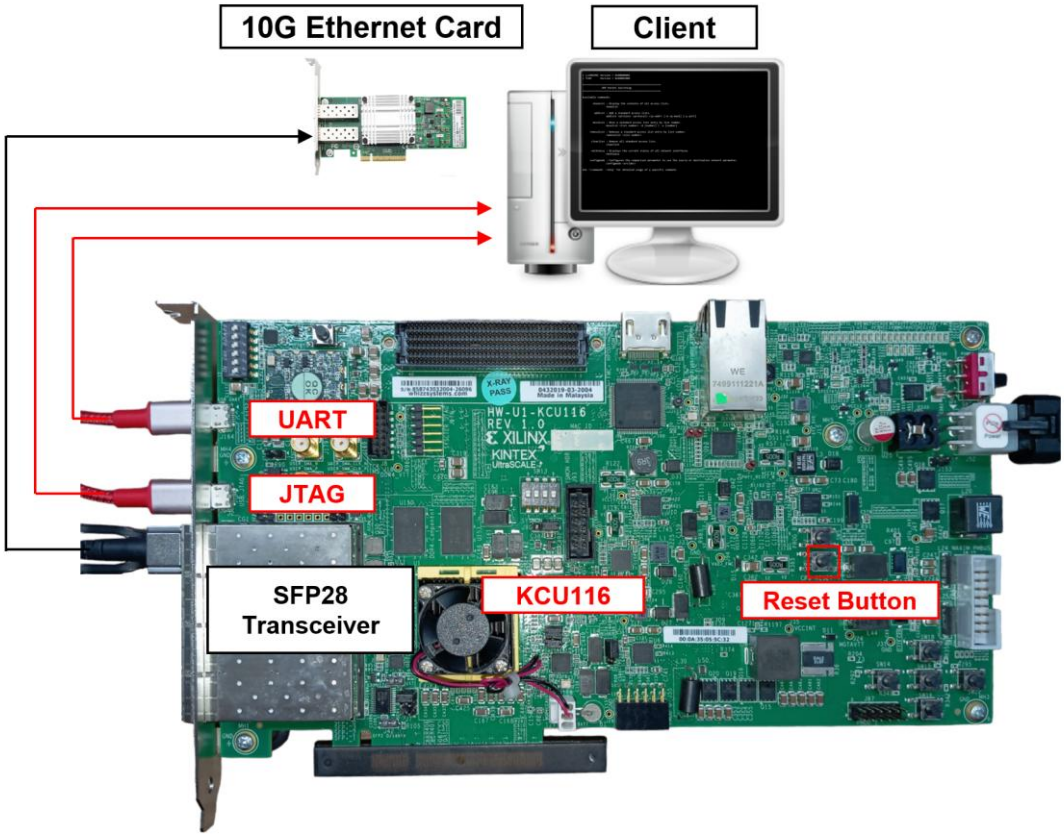

Figure 1 QUIC10GSIP demo environment on KCU116 board

2 PC Setup

Before running demo, please check the network setting on PC. The example of setting 10 Gb Ethernet card is described as follows.

2.1 IP setting

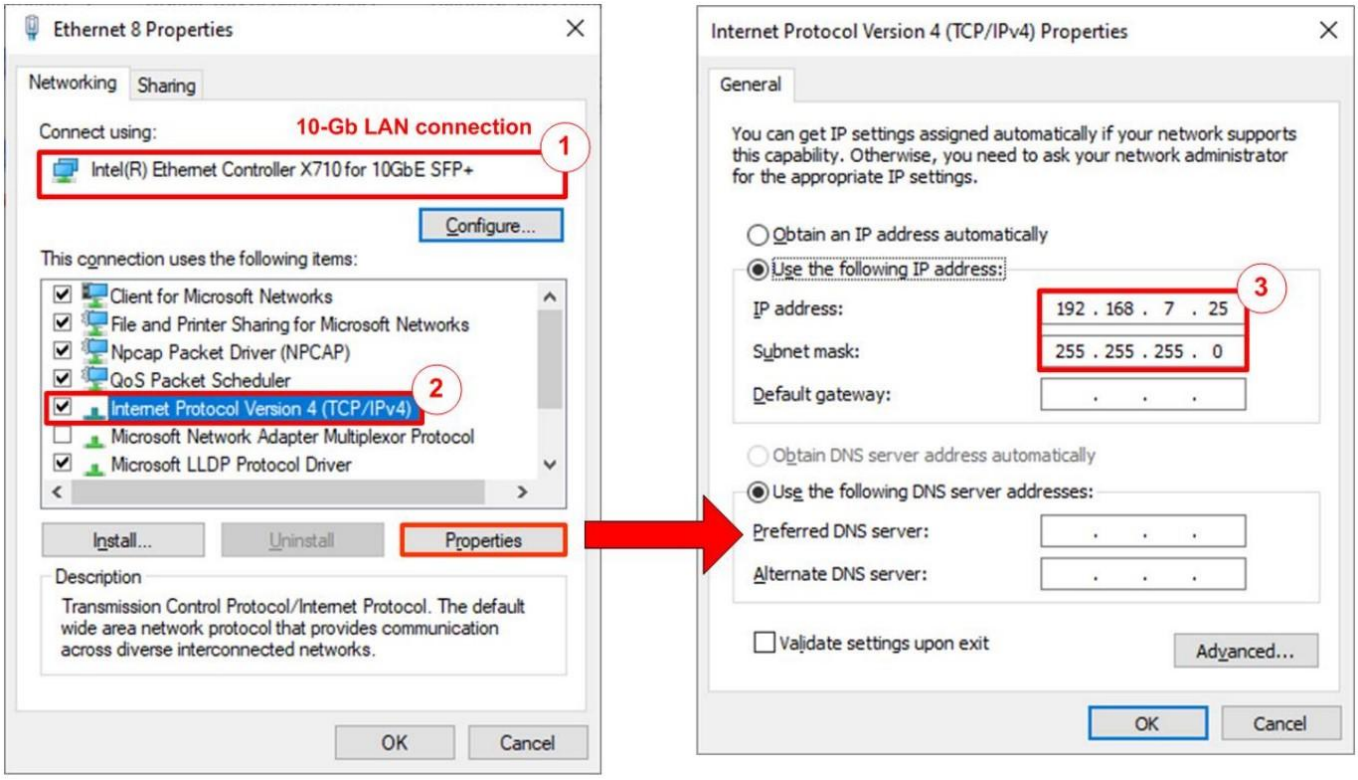

Figure 2 Setting IP address for PC

1) Open Local Area Connection Properties of 10 Gb connection, as shown in the left window of Figure 2.
2) Select “TCP/IPv4” and then click Properties.
3) Set IP address = 192.168.7.25 and Subnet mask = 255.255.255.0, as shown in the right window of Figure 2.

2.2 Speed and duplex settings

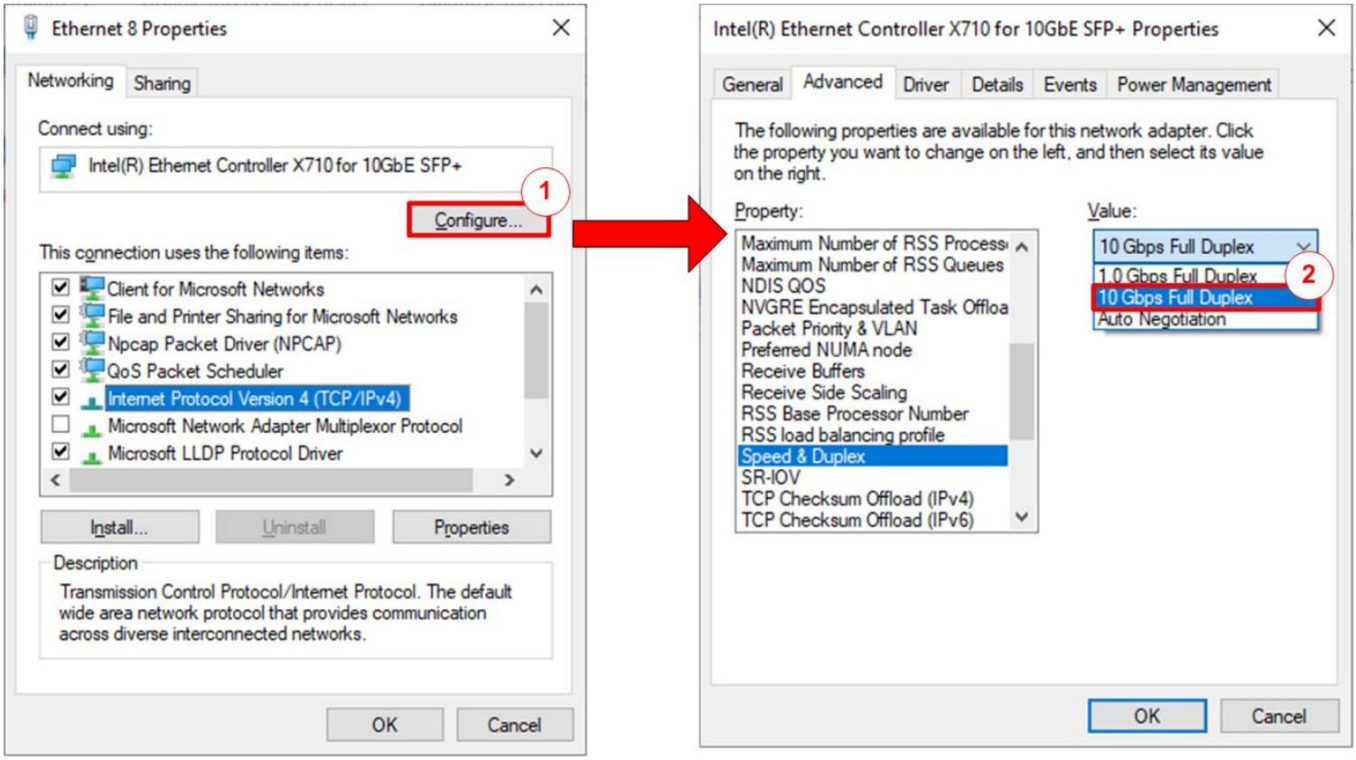

Figure 3 Set Link Speed = 10 Gbps

1) On Local Area Connection Properties window, click “Configure”, as shown in Figure 3.
2) On Advanced Tab, select “Speed and Duplex”. Set the value to “10 Gbps Full Duplex” for running 10 Gigabit transfer test, as shown in Figure 3.

2.3 Network properties settings

Some of network parameter settings may affect network performance. The example of network properties setting is as follows.

1) On “Interrupt Moderation” window, select “Disabled” to disable interrupt moderation which would minimize the latency during transferring data, as shown in Figure 4.

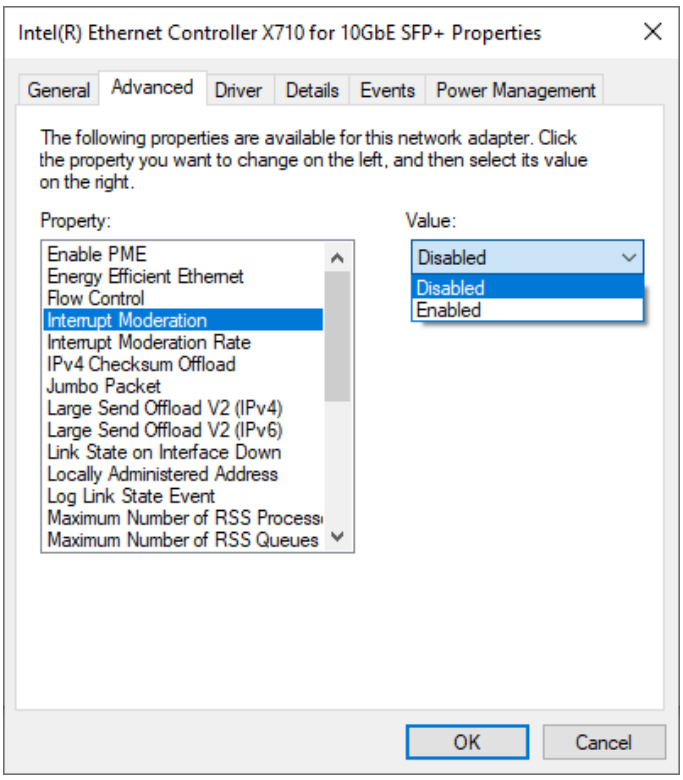

Figure 4 Interrupt Moderation

2) On “Interrupt Moderation Rate” window, set the value to “OFF”, as shown in Figure 5.

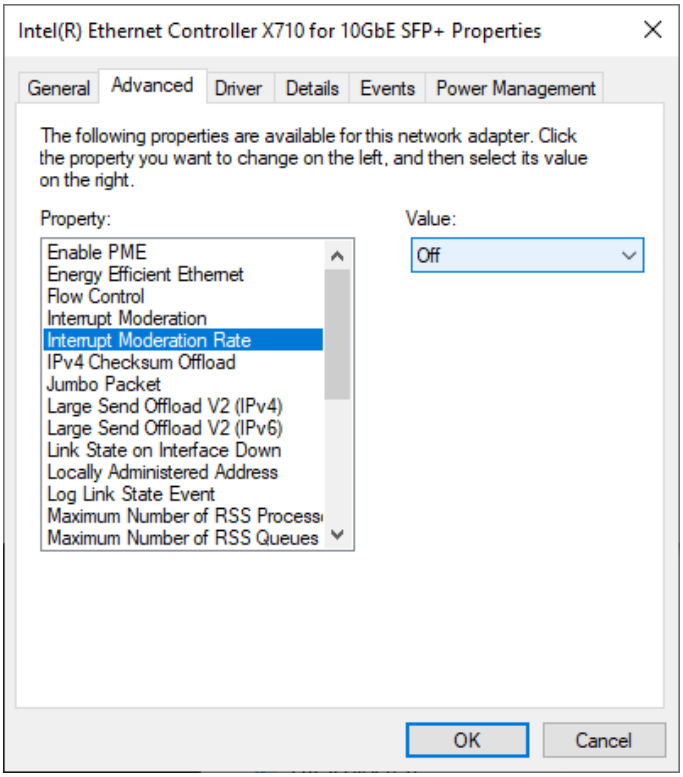

Figure 5 Interrupt Moderation Rate

3) On “Jumbo packet” window, set the value to “9014 Bytes”, as shown in Figure 6.

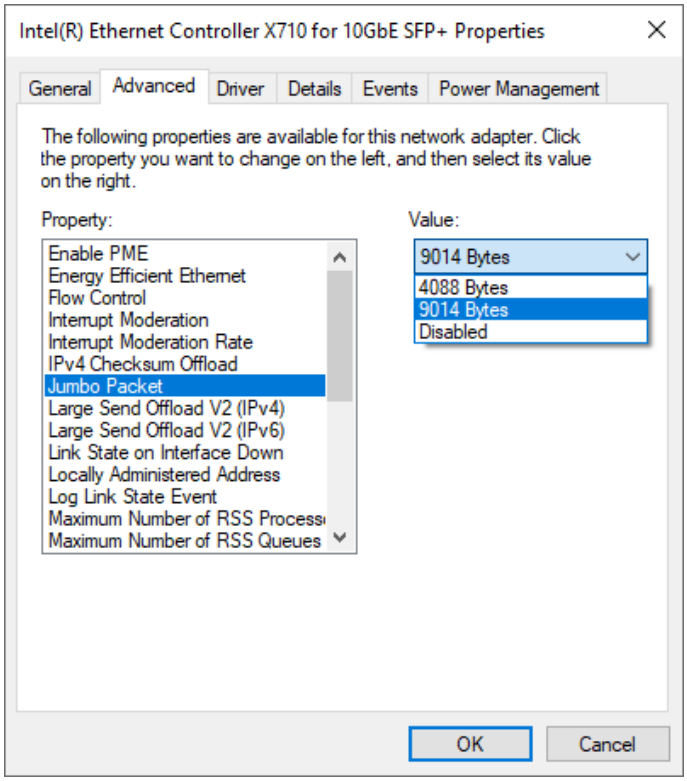

Figure 6 Jumbo packet

4) On “Receive Buffers” window, set the value to the maximum value, as shown in Figure 7.

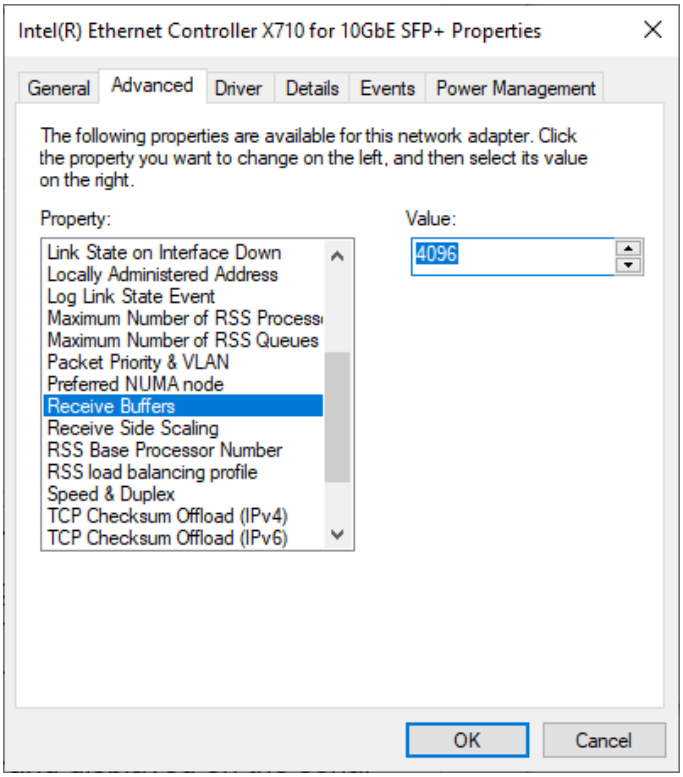

Figure 7 Receive Buffers

5) On “Transmit Buffers” window, set the value to the maximum value, as shown in Figure 8.

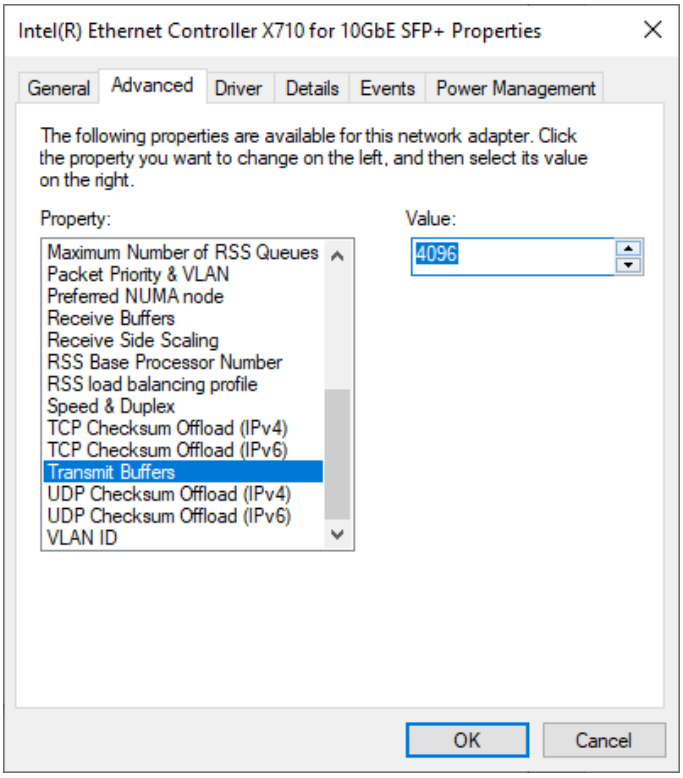

Figure 8 Transmit buffers

3 MsQuic server

QUIC software implementation used in our reference is MsQuic, developed by Microsoft. Their work is an open-source software project, written in C and published in the following website: github.com/microsoft/msquic. We use MsQuic version 2.3.5 and would like to thank Microsoft and the MsQuic team for the development of MsQuic. There is no modification of MsQuic required to run with our demonstration, but we included a folk of MsQuic as a reference branch that we use in this repository: github.com/design-gateway/msquic. If you have any questions regarding their core, please kindly direct them to the MsQuic development team.

There are several application examples offered by MsQuic, but for our reference, an application called 'secnetperf' is applied to run with our demo due to the fact that it is optimized for the high-performance data transfer. For this reason, it uses its own application protocol rather than using the HTTP/3 protocol. Please follow MsQuic's guidelines to set up the application.

To run an MsQuic server using the secnetperf application, secnetperf.exe is called with two options – one is the IP address to bind the server to, and the other is the profile setting of this application, configured for maximum performance in this example. After running the binary file, the message displaying "Started!" is shown as a result, and there will be no other messages thereafter. The example of running the MsQuic is illustrated in Figure 9.

```
PS D:\37.QUIC\folks\msquic> ./artifacts/bin/windows/x64_Debug_openssl/secnetperf.exe -exec:maxtput -ip:192.168.7.25
Started!
```

Figure 9 MsQuic server application console

At this point, a client running the secnetperf application can be connected to the server. To run the client, four options are used in this example: "target" being the IP address of the server to be connected to, "exec" being the same setting as of the server, "up/down" being the length of the upload or download, and "ptput" being the setting to print throughput information. The example of the client console uploading data from the server is shown in Figure 10, while the example of downloading data to the server is shown in Figure 11.

```
PS D:\37.QUIC\folks\msquic> ./artifacts/bin/windows/x64_Debug_openssl/secnetperf -target:192.168.7.25 -up:1gb -ptput:1
-exec:maxtput
Started!

Result: Upload 1000000000 bytes @ 3413934 kbps (2343.337 ms).
```

Figure 10 MsQuic client application console uploading data

```
PS D:\37.QUIC\folks\msquic> ./artifacts/bin/windows/x64_Debug_openssl/secnetperf -target:192.168.7.25 -down:1gb -ptput:1
-exec:maxtput
Started!

Result: Download 1000000000 bytes @ 3593452 kbps (2226.271 ms).
```

Figure 11 MsQuic client application console downloading data

4 FPGA development board setup

1) Make sure the power switch is off and connect the power supply to KCU116 development board.
2) Connect USB cable between PC to JTAG micro-USB port.
3) Power on the system.
4) Open Vivado Hardware Manager to program FPGA by following steps.
    a) Click open Hardware Manager.
    b) Open target -> Auto Connect.
    c) Select FPGA device to program bit file.
    d) Click Program device.
    e) Click "…" to select program bit file.
    f) Click Program button to start FPGA Programming.

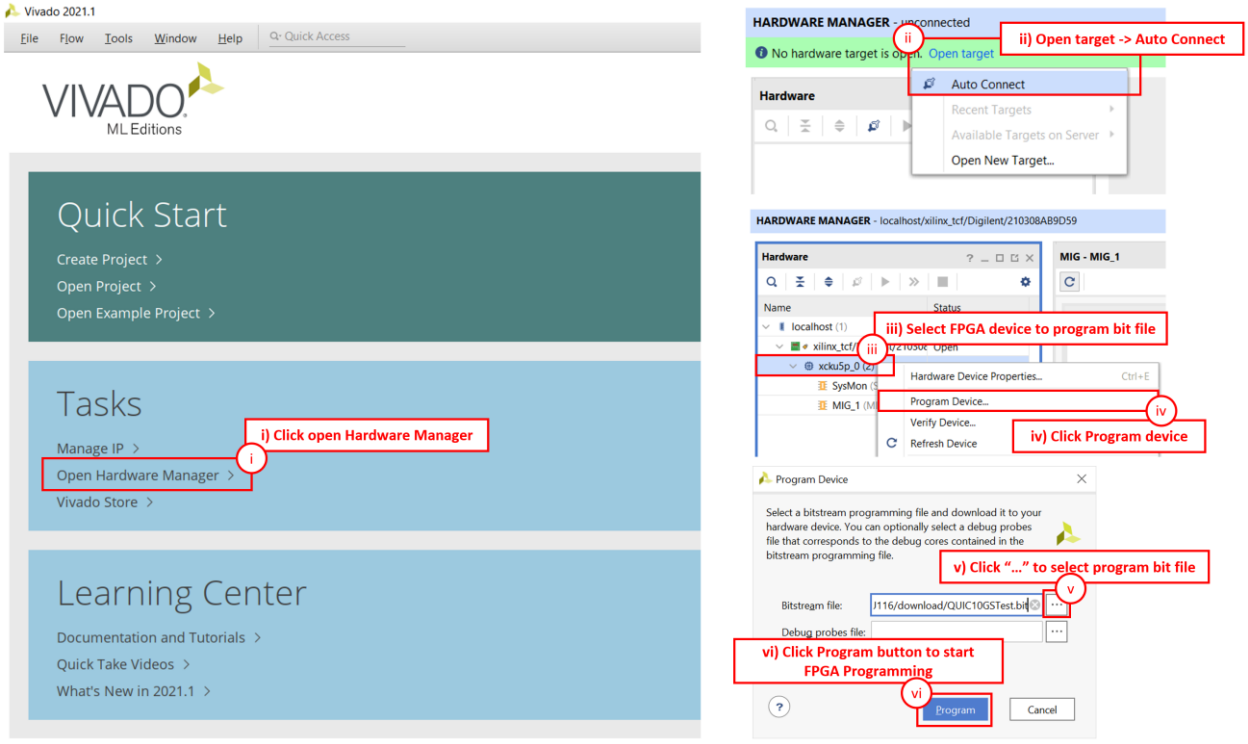

Figure 12 Program Device

5 Serial Console

Users can set the parameters or run the Listen application by using the following commands. The QUIC10GSdemo commands and their usages will be displayed, as shown in Figure 13. Detailed information about each command is described in topic 6.

```
==================================================
            QUIC10GS version 0x80012440
==================================================

Usage:
[0] setip <ddd.ddd.ddd.ddd>
        Set FPGA's IP address in dotted-decimal format.
[1] setport <ddddd>
        Set FPGA's port number in decimal format.
[2] setmac <hh-hh-hh-hh-hh-hh>
        Set FPGA's MAC address in hexadecimal format.
[3] showkey <1: enable, 0: disable>
        Enable showkey mode for showing TLS traffic ticket.
[4] setcert
        Set server's certificate by inputting ASN.1 DER Certificate in binary file via serial console.
[5] setrsakey
        Set server's RSA key information by inputting ASN.1 DER RSA private key in binary file via serial console.
[6] printcert
        Display the server's certificate in hexdump format.
[7] printrsakey
        Display the server's RSA key information in hexdump format.
[8] Listen
        Open server with PERF protocol for both receiving and transmitting pattern data with SecNetPerf of msquic.
        Press 'x' to abort the operation.

>>
```

Figure 13 Serial console

6 Command detail

6.1 Set FPGA's IP Address

command> setip ddd.ddd.ddd.ddd

This command is used to set the FPGA's IP address in dotted-decimal format. The default FPGA's IP address is 192.168.7.42. Users can input the setip command followed by a valid IP address, as shown in Figure 14.

6.2 Set FPGA's Port Number

command> setport ddddd

This command is used to set the static port number of FPGA in decimal format. The default FPGA's Port number is 4433. Users can input the setport command followed by a valid Port number, as shown in Figure 14.

6.3 Set FPGA's MAC address

command> setmac hh-hh-hh-hh-hh-hh

This command is used to set the FPGA's MAC address in hexadecimal format. The default FPGA's MAC address is 80-11-22-33-44-55, which is a unicast MAC address. Users can input the setmac command followed by a valid MAC address, as show in Figure 14.

```
==================================================
            QUIC10GS version 0x80012440
==================================================

Usage:
[0] setip <ddd.ddd.ddd.ddd>
        Set FPGA's IP address in dotted-decimal format.
[1] setport <ddddd>
        Set FPGA's port number in decimal format.
[2] setmac <hh-hh-hh-hh-hh-hh>
        Set FPGA's MAC address in hexadecimal format.
[3] showkey <1: enable, 0: disable>
        Enable showkey mode for showing TLS traffic ticket.
[4] setcert
        Set server's certificate by inputting ASN.1 DER Certificate in binary file via serial console.
[5] setrsakey
        Set server's RSA key information by inputting ASN.1 DER RSA private key in binary file via serial console.
[6] printcert
        Display the server's certificate in hexdump format.
[7] printrsakey
        Display the server's RSA key information in hexdump format.
[8] Listen
        Open server with PERF protocol for both receiving and transmitting pattern data with SecNetPerf of msquic.
        Press 'x' to abort the operation.

>> setip 192.168.7.42
Set FPGA's IP Address to 192.168.7.42

>> setport 4433
Set Port number to 4433

>> setmac 80-11-22-33-44-55
Set FPGA's MAC Address to 80-11-22-33-44-55

>>
```

Figure 14 Serial console when set network parameter

6.4 Enable showkey mode

command> showkey <1: enable, 0: disable>

This command is used to enable the showkey mode. When the showkey mode is enabled, the TLS traffic ticket for encryption/decryption is displayed on the serial console, as shown in Figure 15. Users can utilize the TLS traffic ticket in the (Pre)-Master-Secret log file for Wireshark*, enabling them to decrypt transferred data between the client and server.

*Wireshark, a network packet analyzer tool used for network troubleshooting, analysis, and security purposes.

Figure 15 Serial console when the showkey mode is enabled

6.5 Set certificate

command> setcert

This command is used to set the server's certificate, which must be valid before starting a server. The supported certificate format is ASN.1 DER as a binary file. If the certificate is in PEM format, it must be converted to ASN.1 DER using the following OpenSSL command:

openssl x509 -in <input_file>.pem -out <output_file>.der -outform der

As shown in Figure 16, the output certificate will be in binary format. Users can send the binary certificate file (cert.der) via the serial console as Figure 17. In this demonstration, the maximum supported certificate file size is 8 KB.

```
D:\test>openssl x509 -in cert.pem -out cert.bin -outform der | hexdump -C cert.der
000000  30 82 03 53 30 82 02 3b a0 03 02 01 02 02 14 50  0..SO..;.......P
000010  10 dd bc f4 a8 3c 39 69 76 11 e8 b2 a0 ca 2b c5  .....<9iv.....+.
000020  67 89 8a 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b  g..0...*.H......
000030  05 00 30 38 31 0b 30 09 06 03 55 04 06 13 02 54  ..081.0...U....T
000040  48 31 10 30 0e 06 03 55 04 08 0c 07 42 61 6e 67  H1.0...U....Bang
000050  6b 6f 6b 31 17 30 15 06 03 55 04 0a 0c 0e 44 65  kok1.0...U....De
000060  73 69 67 6e 20 47 61 74 65 77 61 79 30 20 17 0d  sign Gateway0 ..
000070  32 33 30 32 32 34 30 39 32 38 31 30 5a 18 0f 32  230224092810Z..2
000080  31 32 33 30 31 33 31 30 39 32 38 31 30 5a 30 38  1230131092810Z08
000090  31 0b 30 09 06 03 55 04 06 13 02 54 48 31 10 30  1.0...U....TH1.0
0000a0  0e 06 03 55 04 08 0c 07 42 61 6e 67 6b 6f 6b 31  ...U....Bangkok1
0000b0  17 30 15 06 03 55 04 0a 0c 0e 44 65 73 69 67 6e  .0...U....Design
0000c0  20 47 61 74 65 77 61 79 30 82 01 22 30 0d 06 09   Gateway0.."0...
0000d0  2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00  *.H.............
0000e0  30 82 01 0a 02 82 01 01 00 c0 36 8c 0a dc 4f bf  0.........6...O.
0000f0  0b 1c 40 3c 77 17 ef bb 81 f3 c5 02 d2 f7 ca ca  ..@<w...........
000100  96 ca d0 cd 3f 0b 48 c1 87 fc f3 b7 13 5e 29 b6  ....?.H......^).
000110  c9 96 19 f4 ed bc c2 8d eb af f6 92 0a a2 b9 93  ................
000120  5c cf 34 bd 1b 3c d1 24 54 7f 59 6b 75 9f f7 00  \.4..<.$T.Yku...
000130  ee 38 4a 13 60 72 96 23 97 21 6b 01 5a 22 40 94  .8J.`r.#.!k.Z"@.
000140  63 8f 2b 24 4f 07 64 36 d7 af 55 14 b8 98 eb f7  c.+$O.d6..U.....
000150  df 8f 03 07 2e eb 97 e8 64 78 73 17 18 a4 7b 79  ........dxs...{y
000160  2a fb 5e 4d 75 06 c4 43 62 ba c7 5f a9 72 e5 8e  *.^Mu..Cb.._.r..
000170  74 c5 ae b5 fe 98 65 49 d3 7f c0 de 39 31 9d 06  t.....eI....91..
000180  38 ac fa ad 68 64 d0 3a b9 51 d6 24 53 7c 81 67  8...hd.:.Q.$S|.g
000190  fd db 19 a9 a8 95 34 00 7e 83 f1 68 6c 59 ca 49  ......4.~..hlY.I
0001a0  1d 99 d7 34 4c 56 01 2a 83 d1 5c 12 cb c8 83 4b  ...4LV.*..\....K
0001b0  aa 53 58 11 e6 33 c0 bd a2 89 1e 4e 59 75 91 54  .SX..3.....NYu.T
0001c0  78 9d 85 3c fb c8 72 69 1f d1 97 e1 95 aa 25 d2  x..<..ri......%.
0001d0  cb e8 90 a1 53 48 34 29 7d b8 6f b3 80 aa cc 29  ....SH4)}.o....)
0001e0  a8 d5 9c 82 47 db 75 8f 9f 02 03 01 00 01 a3 53  ....G.u........S
0001f0  30 51 30 1d 06 03 55 1d 0e 04 16 04 14 da 27 4c  0Q0...U.......'L
000200  41 24 45 7b 02 d8 58 0b 6c 13 ec 74 f9 6e ff df  A$E{..X.l..t.n..
000210  ae 30 1f 06 03 55 1d 23 04 18 30 16 80 14 da 27  .0...U.#..0....'
000220  4c 41 24 45 7b 02 d8 58 0b 6c 13 ec 74 f9 6e ff  LA$E{..X.l..t.n.
000230  df ae 30 0f 06 03 55 1d 13 01 01 ff 04 05 30 03  ..0...U.......0.
000240  01 01 ff 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b  ...0...*.H......
000250  05 00 03 82 01 01 00 3d c9 31 35 35 85 b8 84 0d  .......=.155....
000260  61 a0 25 c0 47 a8 56 ec a3 a3 09 13 28 50 ee 2c  a.%.G.V.....(P.,
000270  32 35 0f 33 c5 a9 32 42 74 4d 54 28 28 6a c8 d7  25.3..2BtMT((j..
000280  4c b2 80 cc 90 d0 a9 5b 06 e6 60 14 25 91 18 ed  L......[..`.%...
000290  e1 ef 31 42 1e 86 72 f2 4d 1b 9d 14 0c 6f 0c 96  ..1B..r.M....o..
0002a0  de ff d8 9e 85 d6 89 7e 49 a8 59 6a 8a 21 28 f7  .......~I.Yj.!(.
0002b0  36 15 10 e7 11 e3 78 48 4c a2 30 bf b4 93 f0 38  6.....xHL.0....8
0002c0  27 99 ce d1 73 de 42 fc 02 25 3c f2 1f bd aa 32  '...s.B..%<....2
0002d0  02 2f eb 21 cb 78 c0 cf c2 ee 84 e9 bf eb 35 ab  ./.!.x........5.
0002e0  f4 c8 71 6c 23 e8 f5 61 e6 03 8c 2d 43 1c 0a bf  ..ql#..a...-C...
0002f0  e8 e1 99 e8 b2 93 a0 45 da 58 15 ed 35 a2 0a a1  .......E.X..5...
000300  e2 75 ee ea c8 8a 9f b9 d0 46 d9 7a 76 44 fb f1  .u.......F.zvD..
000310  fa 9b ab a8 79 dc 40 7f 15 8d 57 a7 0b d4 30 eb  ....y.@...W...0.
000320  2a 29 ae f6 70 b2 f4 a3 61 5d b8 6c e0 cd fb 51  *)..p...a].l...Q
000330  96 7a 01 18 12 1c 3f 76 c4 84 d2 a8 9e 6f 65 fb  .z....?v.....oe.
000340  07 29 d9 24 c0 fd 10 e4 98 3a b3 ab b4 76 4d c0  .).$.....:...vM.
000350  de 44 00 4e e1 37 62                             .D.N.7b
```

Figure 16 Certificate information from openssl command

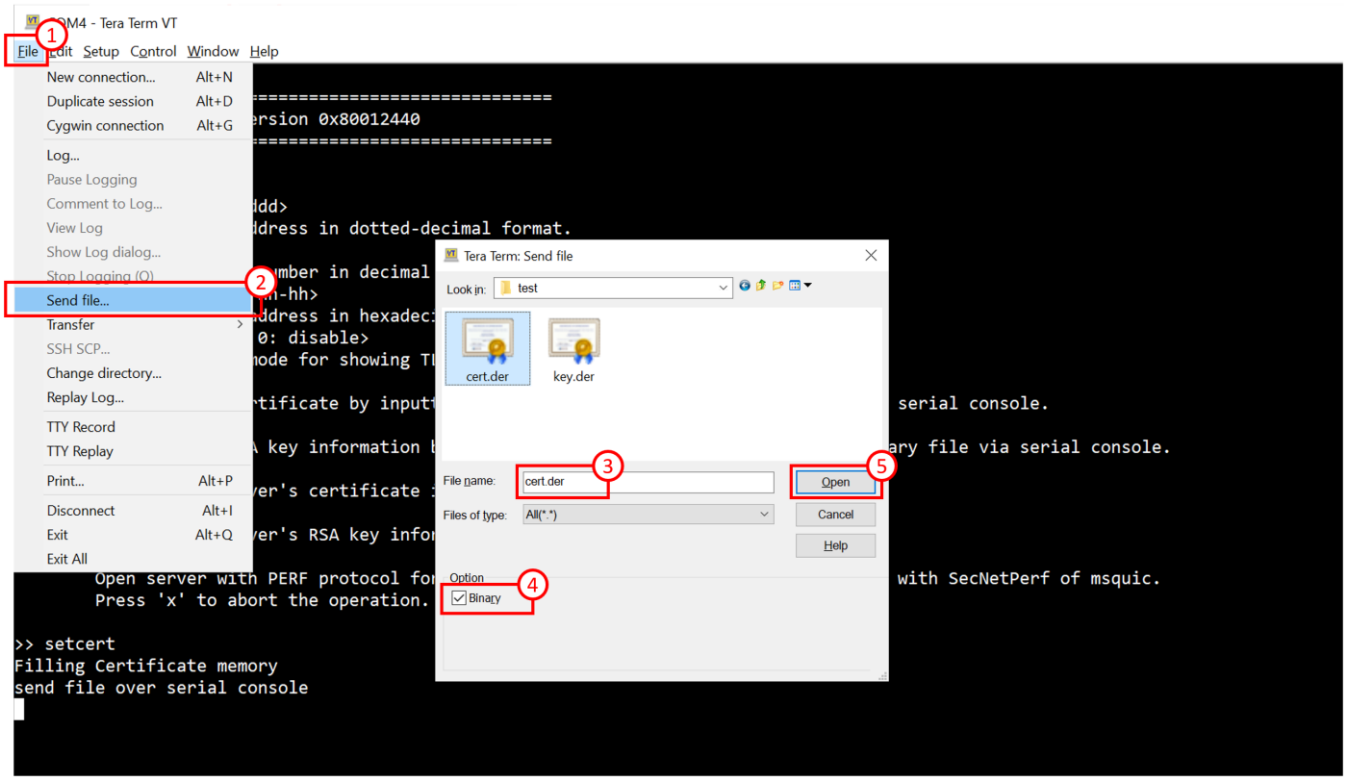

Figure 17 Example binary file transfer

6.6 Set RSA key information

command> setrsakey

This command is used to set RSA key information, which must be valid before starting the server. The supported RSA key format is ASN.1 DER as a binary file. If the RSA key is in PEM format, it must be converted to ASN.1 DER using the following OpenSSL command:

openssl rsa -in <input_file>.pem -out <output_file>.der -outform der

As shown in Figure 18, the output RSA key will be in binary format. Users can send the binary RSA key file (key.der) via the serial console. In this demonstration, the maximum supported RSA key size is 2 KB.


```
D:\test>openssl rsa -in key.pem -out key.der -outform der | hexdump -C key.der
writing RSA key
00000000  30 82 04 be 02 01 00 30  0d 06 09 2a 86 48 86 f7  |0......0...*.H..|
00000010  0d 01 01 01 05 00 04 82  04 a8 30 82 04 a4 02 01  |..........0.....|
00000020  00 02 82 01 01 00 c0 36  8c 0a dc 4f bf 0b 1c 40  |.......6...O...@|
00000030  3c 77 17 ef bb 81 f3 c5  02 d2 f7 ca ca 96 ca d0  |<w..............|
00000040  cd 3f 0b 48 c1 87 fc f3  b7 13 5e 29 b6 c9 96 19  |.?.H......^)....|
00000050  f4 ed bc c2 8d eb af f6  92 0a a2 b9 93 5c cf 34  |.............\.4|
00000060  bd 1b 3c d1 24 54 7f 59  6b 75 9f f7 00 ee 38 4a  |..<.$T.Yku....8J|
00000070  13 60 72 96 23 97 21 6b  01 5a 22 40 94 63 8f 2b  |.`r.#.!k.Z"@.c.+|
00000080  24 4f 07 64 36 d7 af 55  14 b8 98 eb f7 df 8f 03  |$O.d6..U........|
00000090  07 2e eb 97 e8 64 78 73  17 18 a4 7b 79 2a fb 5e  |.....dxs...{y*.^|
000000a0  4d 75 06 c4 43 62 ba c7  5f a9 72 e5 8e 74 c5 ae  |Mu..Cb.._.r..t..|
000000b0  b5 fe 98 65 49 d3 7f c0  de 39 31 9d 06 38 ac fa  |...eI....91..8..|
000000c0  ad 68 64 d0 3a b9 51 d6  24 53 7c 81 67 fd db 19  |.hd.:.Q.$S|.g...|
000000d0  a9 a8 95 34 00 7e 83 f1  68 6c 59 ca 49 1d 99 d7  |...4.~..hlY.I...|
000000e0  34 4c 56 01 2a 83 d1 5c  12 cb c8 83 4b aa 53 58  |4LV.*..\....K.SX|
000000f0  11 e6 33 c0 bd a2 89 1e  4e 59 75 91 54 78 9d 85  |..3.....NYu.Tx..|
00000100  3c fb c8 72 69 1f d1 97  e1 95 aa 25 d2 cb e8 90  |<..ri......%....|
00000110  a1 53 48 34 29 7d b8 6f  b3 80 aa cc 29 a8 d5 9c  |.SH4)}.o....)...|
00000120  82 47 db 75 8f 9f 02 03  01 00 01 02 82 01 00 2d  |.G.u...........-|
00000130  c6 0f ad 9a 6f a7 48 47  0f 09 17 37 6d 10 d3 4e  |....o.HG...7m..N|
00000140  b1 11 0e 1a 92 81 92 4d  74 52 1c 7c 5c 74 32 25  |.......MtR.|\t2%|
00000150  4c 08 c2 24 ff 7c 17 1f  96 c8 dc 40 c2 78 37 b3  |L..$.|.....@.x7.|
00000160  6c dd b4 88 b1 f6 e4 f8  37 4f fd 87 8b 2a c2 b0  |l.......7O...*..|
00000170  9d 23 d9 1c 22 1f 67 9b  a2 10 61 3c 88 82 ab 3f  |.#..".g...a<...?|
00000180  fb 12 94 5b 69 d3 ac ad  f0 91 31 fc c9 a1 c1 d5  |...[i.....1.....|
00000190  70 46 81 fb 70 de 53 af  e4 01 b6 eb c5 fe 42 c6  |pF..p.S.......B.|
000001a0  e8 69 8c a5 c6 fd c0 fd  a1 a4 82 84 fd 02 2a bc  |.i............*.|
000001b0  33 08 62 39 2c 22 32 2c  aa 3d 24 5b 19 5d 94 6e  |3.b9,"2,.=$[.].n|
000001c0  6f aa 14 31 36 e2 e2 62  40 54 04 d7 0c 42 eb 00  |o..16..b@T...B..|
000001d0  75 80 76 ba 20 2d 80 f3  65 34 3c 67 ec bf 42 27  |u.v. -..e4<g..B'|
000001e0  da 2f 36 d3 7c 56 2f 38  d8 fd a4 6a c8 87 7e ae  |./6.|V/8...j..~.|
000001f0  09 6a 74 a4 05 38 74 12  37 27 26 c4 de 35 0e 3b  |.jt..8t.7'&..5.;|
00000200  b1 c8 75 e6 c1 17 55 f1  10 4d fd 48 5a a0 73 eb  |..u...U..M.HZ.s.|
00000210  93 d3 0d 81 3e ad 00 92  a2 9f 31 3f ad c9 43 7a  |....>.....1?..Cz|
00000220  af d7 70 ba 07 5e cb 7d  c8 db 33 5b bc 13 91 02  |..p..^.}..3[....|
00000230  81 81 00 e1 b3 db c9 71  98 0b 2b 75 bb 11 9c bd  |.......q..+u....|
00000240  22 73 89 3c 22 51 5d b3  ed 8c fe fb af 3c a0 e5  |"s.<"Q].....<..|
00000250  56 12 a5 46 57 4f 88 a4  a5 5a 4f f0 49 23 13 f0  |V..FWO...ZO.I#..|
00000260  97 32 8c c6 66 f2 c9 b4  82 1a f7 f0 aa b2 d5 c0  |.2..f...........|
00000270  e8 50 67 87 bb 2f a2 cc  58 51 cb d1 45 46 91 82  |.Pg../..XQ..EF..|
00000280  43 00 dc b1 4d f5 b4 c6  da 8a 96 65 bb d5 e6 52  |C...M......e...R|
00000290  ee 60 35 24 fa 94 db 13  39 7c 96 46 6a 99 9b ea  |.`5$....9|.Fj...|
000002a0  3f 50 d0 83 2c 25 71 de  9d c2 fb 8c d0 0c c4 f9  |?P..,%q.........|
000002b0  08 58 29 02 81 81 00 da  03 d7 3f 2a 62 dd 05 85  |.X).......?*b...|
000002c0  7b e7 75 d9 00 86 82 7e  35 7b 31 9e 25 3e a5 6c  |{.u....~5{1.%>.l|
000002d0  af a4 33 19 90 77 0d ce  3d 1f 5b 2d d4 27 3f d6  |..3..w..=.[-.'?.|
000002e0  cc ec 51 5b 0f 36 2f b1  3b ac e1 4f 43 32 fe 42  |..Q[.6/.;..OC2.B|
000002f0  b3 93 55 ef 04 c5 31 81  15 c8 5f 8c b6 64 94 e5  |..U...1..._..d..|
00000300  b7 a3 29 52 e1 30 7c ef  ae 07 63 76 06 96 54 2d  |..)R.0|...cv..T-|
00000310  be 7e 6e 92 02 52 ea e7  46 80 6c e6 8a 35 e8 7a  |.~n..R..F.l..5.z|
00000320  e8 dd d7 80 9d 7c 4a 87  6f e8 00 80 c2 57 79 42  |.....|J.o....WyB|
00000330  e3 4e fa 33 40 c2 87 02  81 81 00 9c 91 df 7b 0b  |.N.3@.........{.|
00000340  e1 14 86 8e 82 3a 02 88  35 d8 fe 2f 88 02 f7 c4  |.....:..5../....|
00000350  b4 9a e5 db 84 c1 c3 3f  b4 88 f4 bc 2a 1f 53 44  |.......?....*.SD|
00000360  1c 2c dd 5d 6b ee f8 8b  22 e7 ff 3e 36 f6 5f b4  |.,.]k..."..>6._.|
00000370  67 b8 fb 9c a9 5d ab e8  c9 7f d5 82 13 f9 44 af  |g....]........D.|
00000380  0a e9 9b 41 4e 14 59 26  8b 02 93 16 30 65 ad 85  |...AN.Y&....0e..|
00000390  70 df 48 db c4 04 eb 65  46 55 d9 28 10 e8 a8 5c  |p.H....eFU.(...\|
000003a0  da b9 31 aa 21 92 f3 d4  f9 1d 3f b8 6f 2c 7e a4  |..1.!.....?.o,~.|
000003b0  96 be 47 30 74 b7 17 01  46 a7 99 02 81 81 00 97  |..G0t...F.......|
000003c0  74 03 9c 45 fd d8 3d 75  b5 d5 dd f0 9a 84 d7 32  |t..E..=u.......2|
000003d0  86 44 c6 fb 6e 34 4f 07  6a 1d 4f c2 7a b1 ba 4d  |.D..n4O.j.O.z..M|
000003e0  83 f8 bc 86 e1 d3 42 6e  1e 7e 2d 26 6d 32 df 7e  |......Bn.~-&m2.~|
000003f0  e8 4d f9 57 ee ff 05 d3  a0 9c c2 1e 01 da 5b c1  |.M.W..........[.|
00000400  a9 38 41 e8 a6 ec c8 e3  ac e7 14 56 17 4a 70 00  |.8A........V.Jp.|
00000410  b1 8d 40 73 45 b0 39 5a  6d f3 b7 2c 87 a0 c2 bf  |..@sE.9Zm..,....|
00000420  58 22 ef 84 58 8f 8a a9  98 0c 45 21 7c 46 54 20  |X"..X.....E!|FT |
00000430  32 85 a1 93 d1 6e a3 36  ec 62 79 3e 11 c7 11 02  |2....n.6.by>....|
00000440  81 80 6c 0f eb d1 9c 88  99 3f b4 94 bf 4b 73 00  |..l......?...Ks.|
00000450  5e a7 71 9b da cc 50 b1  48 9f 78 47 c4 77 c4 16  |^.q...P.H.xG.w..|
00000460  5f 34 0f 7c 0a 04 34 20  b5 fa fc 9a 91 74 75 ba  |_4.|..4 .....tu.|
00000470  39 ac f6 bf f5 32 5d f5  79 72 69 22 ba f9 85 3e  |9....2].yri"...>|
00000480  13 a4 72 31 ea ea cf 43  da 8b 0e b4 c0 72 d5 f3  |..r1...C.....r..|
00000490  55 0e df e9 17 df 2c eb  89 70 a3 b6 fb 67 96 fa  |U.....,..p...g..|
000004a0  dc cd 44 78 5e 80 47 e9  36 3c c3 d3 21 78 35 2d  |..Dx^.G.6<..!x5-|
000004b0  ed 9d 9d 97 ee 3c cd b1  93 b4 59 47 5d 0b c6 12  |.....<....YG]...|
000004c0  a5 b4                                             |..|
```

Figure 18 RSA key information from openssl command

6.7 Print certificate

command> printcert

This command is used to display the server's certificate. The output is in ASN.1 DER format and shown in a structured hexadecimal representation. This helps to ensure that the certificate is correctly set and valid before the server starts.

```
>> printcert

Certificate information

00000000  30 82 03 53 30 82 02 3B  A0 03 02 01 02 02 14 50  |0..S0..;.......P|
00000010  10 DD BC F4 A8 3C 39 69  76 11 E8 B2 A0 CA 2B C5  |.....<9iv.....+.|
00000020  67 89 8A 30 0D 06 09 2A  86 48 86 F7 0D 01 01 0B  |g..0...*.H......|
00000030  05 00 30 38 31 0B 30 09  06 03 55 04 06 13 02 54  |..081.0...U....T|
00000040  48 31 10 30 0E 06 03 55  04 08 0C 07 42 61 6E 67  |H1.0...U....Bang|
00000050  6B 6F 6B 31 17 30 15 06  03 55 04 0A 0C 0E 44 65  |kok1.0...U....De|
00000060  73 69 67 6E 20 47 61 74  65 77 61 79 30 20 17 0D  |sign Gateway0 ..|
00000070  32 33 30 32 32 34 30 39  32 38 31 30 5A 18 0F 32  |230224092810Z..2|
00000080  31 32 33 30 31 33 31 30  39 32 38 31 30 5A 30 38  |1230131092810Z08|
00000090  31 0B 30 09 06 03 55 04  06 13 02 54 48 31 10 30  |1.0...U....TH1.0|
000000A0  0E 06 03 55 04 08 0C 07  42 61 6E 67 6B 6F 6B 31  |...U....Bangkok1|
000000B0  17 30 15 06 03 55 04 0A  0C 0E 44 65 73 69 67 6E  |.0...U....Design|
000000C0  20 47 61 74 65 77 61 79  30 82 01 22 30 0D 06 09  | Gateway0.."0...|
000000D0  2A 86 48 86 F7 0D 01 01  01 05 00 03 82 01 0F 00  |*.H.............|
000000E0  30 82 01 0A 02 82 01 01  00 C0 36 8C 0A DC 4F BF  |0.........6...O.|
000000F0  0B 1C 40 3C 77 17 EF BB  81 F3 C5 02 D2 F7 CA CA  |..@<w...........|
00000100  96 CA D0 CD 3F 0B 48 C1  87 FC F3 B7 13 5E 29 B6  |....?.H......^).|
00000110  C9 96 19 F4 ED BC C2 8D  EB AF F6 92 0A A2 B9 93  |................|
00000120  5C CF 34 BD 1B 3C D1 24  54 7F 59 6B 75 9F F7 00  |\.4..<.$T.Yku...|
00000130  EE 38 4A 13 60 72 96 23  97 21 6B 01 5A 22 40 94  |.8J.`r.#.!k.Z"@.|
00000140  63 8F 2B 24 4F 07 64 36  D7 AF 55 14 B8 98 EB F7  |c.+$O.d6..U.....|
00000150  DF 8F 03 07 2E EB 97 E8  64 78 73 17 18 A4 7B 79  |........dxs...{y|
00000160  2A FB 5E 4D 75 06 C4 43  62 BA C7 5F A9 72 E5 8E  |*.^Mu..Cb.._.r..|
00000170  74 C5 AE B5 FE 98 65 49  D3 7F C0 DE 39 31 9D 06  |t.....eI....91..|
00000180  38 AC FA AD 68 64 D0 3A  B9 51 D6 24 53 7C 81 67  |8...hd.:.Q.$S|.g|
00000190  FD DB 19 A9 A8 95 34 00  7E 83 F1 68 6C 59 CA 49  |......4.~..hlY.I|
000001A0  1D 99 D7 34 4C 56 01 2A  83 D1 5C 12 CB C8 83 4B  |...4LV.*..\....K|
000001B0  AA 53 58 11 E6 33 C0 BD  A2 89 1E 4E 59 75 91 54  |.SX..3.....NYu.T|
000001C0  78 9D 85 3C FB C8 72 69  1F D1 97 E1 95 AA 25 D2  |x..<..ri......%.|
000001D0  CB E8 90 A1 53 48 34 29  7D B8 6F B3 80 AA CC 29  |....SH4)}.o....)|
000001E0  A8 D5 9C 82 47 DB 75 8F  9F 02 03 01 00 01 A3 53  |....G.u........S|
000001F0  30 51 30 1D 06 03 55 1D  0E 04 16 04 14 DA 27 4C  |0Q0...U.......'L|
00000200  41 24 45 7B 02 D8 58 0B  6C 13 EC 74 F9 6E FF DF  |A$E{..X.l..t.n..|
00000210  AE 30 1F 06 03 55 1D 23  04 18 30 16 80 14 DA 27  |.0...U.#..0....'|
00000220  4C 41 24 45 7B 02 D8 58  0B 6C 13 EC 74 F9 6E FF  |LA$E{..X.l..t.n.|
00000230  DF AE 30 0F 06 03 55 1D  13 01 01 FF 04 05 30 03  |..0...U.......0.|
00000240  01 01 FF 30 0D 06 09 2A  86 48 86 F7 0D 01 01 0B  |...0...*.H......|
00000250  05 00 03 82 01 01 00 3D  C9 31 35 35 85 B8 84 0D  |.......=.155....|
00000260  61 A0 25 C0 47 A8 56 EC  A3 A3 09 13 28 50 EE 2C  |a.%.G.V.....(P.,|
00000270  32 35 0F 33 C5 A9 32 42  74 4D 54 28 28 6A C8 D7  |25.3..2BtMT((j..|
00000280  4C B2 80 CC 90 D0 A9 5B  06 E6 60 14 25 91 18 ED  |L......[..`.%...|
00000290  E1 EF 31 42 1E 86 72 F2  4D 1B 9D 14 0C 6F 0C 96  |..1B..r.M....o..|
000002A0  DE FF D8 9E 85 D6 89 7E  49 A8 59 6A 8A 21 28 F7  |.......~I.Yj.!(.|
000002B0  36 15 10 E7 11 E3 78 48  4C A2 30 BF B4 93 F0 38  |6.....xHL.0....8|
000002C0  27 99 CE D1 73 DE 42 FC  02 25 3C F2 1F BD AA 32  |'...s.B..%<....2|
000002D0  02 2F EB 21 CB 78 C0 CF  C2 EE 84 E9 BF EB 35 AB  |./.!.x........5.|
000002E0  F4 C8 71 6C 23 E8 F5 61  E6 03 8C 2D 43 1C 0A BF  |..ql#..a...-C...|
000002F0  E8 E1 99 E8 B2 93 A0 45  DA 58 15 ED 35 A2 0A A1  |.......E.X..5...|
00000300  E2 75 EE EA C8 8A 9F B9  D0 46 D9 7A 76 44 FB F1  |.u.......F.zvD..|
00000310  FA 9B AB A8 79 DC 40 7F  15 8D 57 A7 0B D4 30 EB  |....y.@...W...0.|
00000320  2A 29 AE F6 70 B2 F4 A3  61 5D B8 6C E0 CD FB 51  |*)..p...a].l...Q|
00000330  96 7A 01 18 12 1C 3F 76  C4 84 D2 A8 9E 6F 65 FB  |.z....?v.....oe.|
00000340  07 29 D9 24 C0 FD 10 E4  98 3A B3 AB B4 76 4D C0  |.).$.....:...vM.|
00000350  DE 44 00 4E E1 37 62                              |.D.N.7b         |
```

Figure 19 Serial console when print certificate

6.8 Print RSA key information

command> printrsakey

This command is used to show the server's rsa key. The output is in ASN.1 DER format and shown in a structured hexadecimal representation. This helps to ensure that the rsa key is correctly set and valid before the server starts.

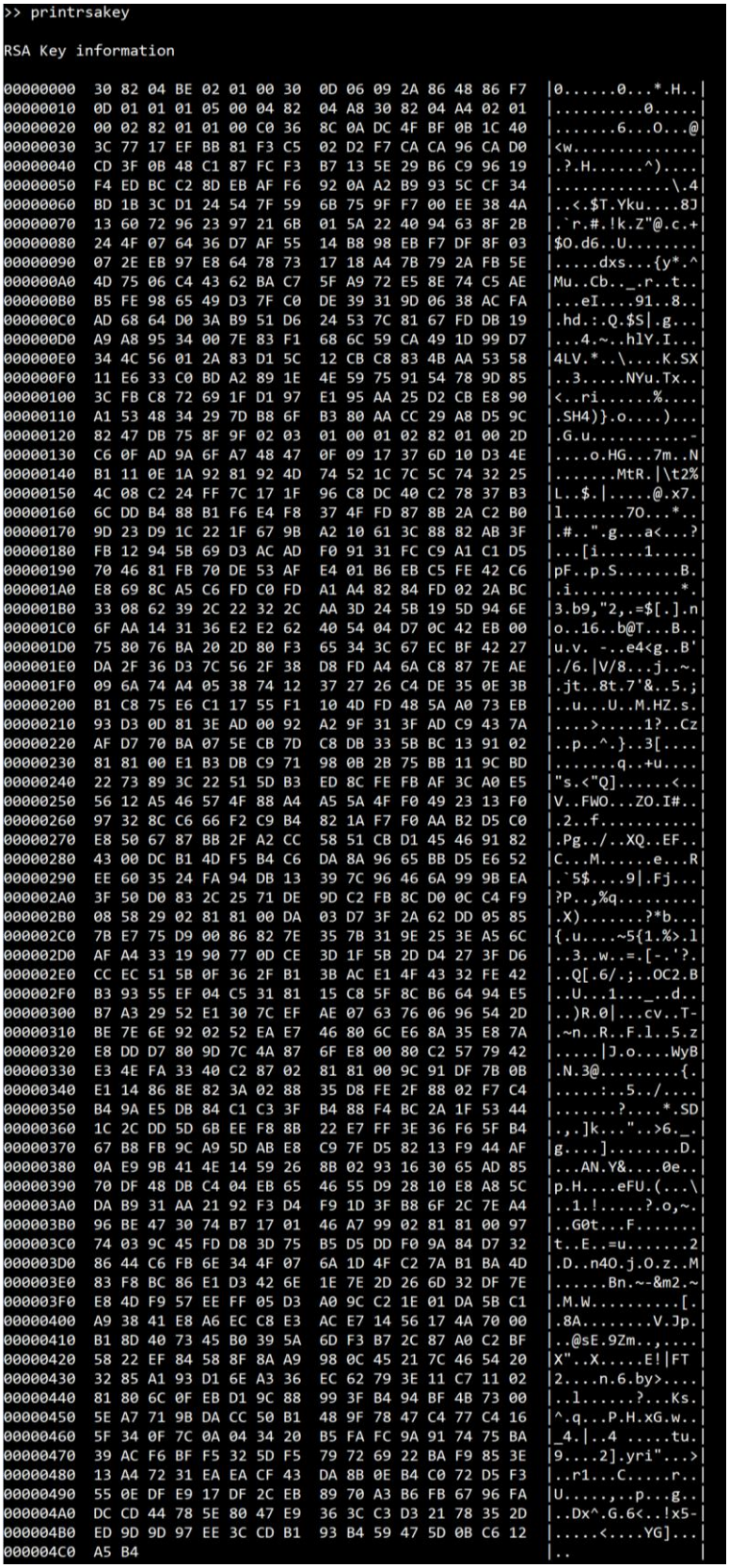

Figure 20 Serial console when print rsa key

6.9 Start a server

Command> listen

The listen command is used to run the 'secnetperf' example of an MsQuic client. The server listens for incoming connections on the FPGA IP address and port number. When a connection is established by the client, the server responds to incoming data based on supported requests from the client.

The verification feature is enabled to monitor the received data. The results, including download content, transfer length, and transfer speed, are presented (see Figure 21). It's important to note that the performance of this operation depends on the network system and available resources on the test machine.

```
>> Listen
Listen on 192.168.7.42:4433
=========================================
Connection from 192.168.7.25:50293
Handshake done
Running...done
Connection closed 192.168.7.25:50293
=========================================
Pattern data has been verified, and
Showing Rx data content with the first data offset at 0x00029BF4

Address    0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00029BF0  F0 F1 F2 F3 00 00 00 00 00 00 01 F4 08 09 0A 0B
00029C00  0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
00029C10  1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B
00029C20  2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B
00029C30  3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B
00029C40  4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B
00029C50  5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69 6A 6B
00029C60  6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B
00029C70  7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89 8A 8B
00029C80  8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99 9A 9B
00029C90  9C 9D 9E 9F A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB
00029CA0  AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB
00029CB0  BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB
00029CC0  CC CD CE CF D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB
00029CD0  DC DD DE DF E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB
00029CE0  EC ED EE EF F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB
00029CF0  FC FD FE FF 00 01 02 03 04 05 06 07 08 09 0A 0B
00029D00  0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B
00029D10  1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B
00029D20  2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B
00029D30  3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B
00029D40  4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B
00029D50  5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69 6A 6B
00029D60  6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B
00029D70  7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89 8A 8B
00029D80  8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99 9A 9B
00029D90  9C 9D 9E 9F A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB
00029DA0  AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB
00029DB0  BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB
00029DC0  CC CD CE CF D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB
00029DD0  DC DD DE DF E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB
00029DE0  EC ED EE EF F0 F1 F2 F3 E8 E9 EA EB EC ED EE EF

=========================================
Total transfer size = 500 Byte(s)
Transmitting Speed 1.230 Mbps
Total transfer size = 500 Byte(s)
Receiving Speed 121.212 Mbps
=========================================
```

Figure 21 Serial console when downloading small data

However, Figure 21 may not be ideal for representing transfer performance because the operation time is too short for accurate calculations. Figure 22 shows transfer speed for server receiving, while Figure 23 presents speed for server transmitting. Figure 24 provides transfer speed for both transmitting and receiving, as the transfer size settings are large enough for meaningful results.

```
>> Listen
Listen on 192.168.7.42:4433
==========================================
Connection from 192.168.7.25:62557
Handshake done
Running...done
Connection closed 192.168.7.25:62557
==========================================
Pattern data has been verified, and
Data content is too large so only the transfer speed is displayed
==========================================
Total transfer size = 0 Byte(s)
Transmitting Speed 0 bps
Total transfer size = 8000000000 Byte(s)
Receiving Speed 8.867 Gbps
==========================================
```

Figure 22 Serial console display during server receiving large data

```
>> Listen
Listen on 192.168.7.42:4433
==========================================
Connection from 192.168.7.25:55966
Handshake done
Running...done
Connection closed 192.168.7.25:55966
==========================================
Pattern data has been verified, and
Showing Rx data content with the first data offset at 0x0000EDE8

Address    0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
0000EDE0  F8 F9 FA FB FC FD FE FF 00 00 00 01 DC D6 50 00
0000EDF0  08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17

==========================================
Total transfer size = 8000000000 Byte(s)
Transmitting Speed 3.621 Gbps
Total transfer size = 8 Byte(s)
Receiving Speed 4.571 Mbps
==========================================
```

Figure 23 Serial console display during server transmitting large data

```
>> Listen
Listen on 192.168.7.42:4433
==========================================
Connection from 192.168.7.25:56114
Handshake done
Running...done
Connection closed 192.168.7.25:56114
==========================================
Pattern data has been verified, and
Data content is too large so only the transfer speed is displayed
==========================================
Total transfer size = 8000000000 Byte(s)
Transmitting Speed 2.673 Gbps
Total transfer size = 8000000000 Byte(s)
Receiving Speed 2.634 Gbps
==========================================
```

Figure 24 Serial console display during server transmitting and receiving large data

7 Test setup when using 2 FPGA boards

This test setup evaluates performance between two FPGA boards using the QUIC10GC-IP as the client and the QUIC10GS-IP as the server, ensuring no bottleneck from CPU software. The test utilizes a secure connection over the QUIC transport protocol, enabling high-speed data transfer with hardware acceleration. At the application layer, a dedicated protocol—similar to MsQuic's 'secnetperf' example—is implemented to measure performance. This setup enables a fully hardware-driven QUIC communication, independent of software processing constraints.

7.1 Environment setup when using 2 FPGA boards

To operate QUIC10GS-IP demo with QUIC10GC-IP demo, please prepare following test environment.

1) FPGA development boards (KCU116 as a server and ZCU106 as a client).
2) 10 Gb Ethernet cable:
    a) 10 Gb SFP+ Passive Direct Attach Cable (DAC) which has 1-m or less length
    b) 10 Gb SFP+ Active Optical Cable (AOC)
    c) 2x10 Gb SFP+ transceiver (10G BASE-R) with optical cable (LC to LC, Multimode)
3) Micro USB cable for JTAG connection connecting between FPGA board and Test PC.
4) 2 Micro USB cable for UART connection connecting between KCU116 board and Test PC and between ZCU106 board and Test PC.
5) Vivado tool for programming FPGA installed on Test PC.
6) Serial console software such as TeraTerm installed on PC. The setting on the console is Baudrate=115200, Data=8-bit, Non-parity and Stop=1.
7) Batch file named "QUIC10GSIPTest.bit" and "QUIC10GCIPTest.bat" (To download these files, please visit our website at www.design-gateway.com)

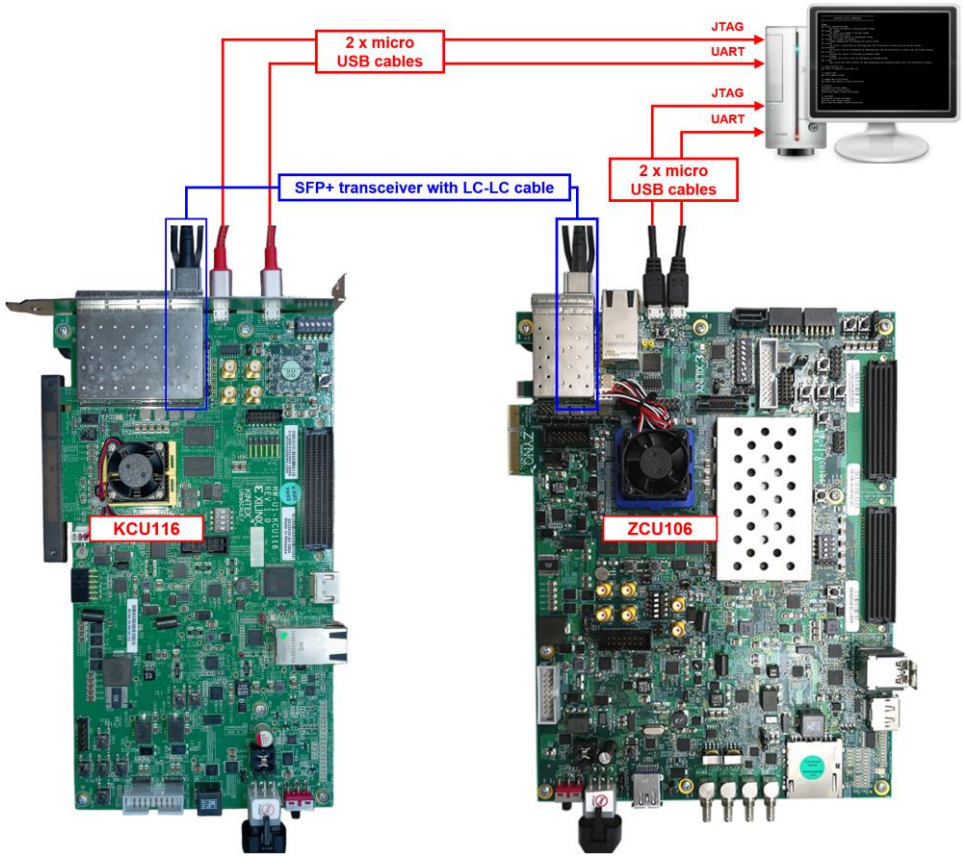

Figure 25 QUIC10GS-IP demo environment when using 2 FPGA boards

Follow step 1)-4) of Topic 4 Board setup to prepare FPGA boards for running the demo. Run "QUIC10GSTest.bit" to download configuration file and firmware to KCU116 board as a server and run "QUIC10GCTest.bat" to download configuration file and firmware to ZCU106 board as a client. The details of supported commands and their usage for QUIC10GC-IP demo is described in the following link.

https://dgway.com/products/IP/QUIC-IP/QUIC10GCIP-instruction-xilinx-en/

7.2 Test sequence

7.2.1 Set parameters and start a server

1) Set network parameters of each FPGA board: IP address, port number, and Mac address.
2) Set server's certificate and RSA key information via serial console of server.
3) Start the server, allowing it to listen for incoming connections.

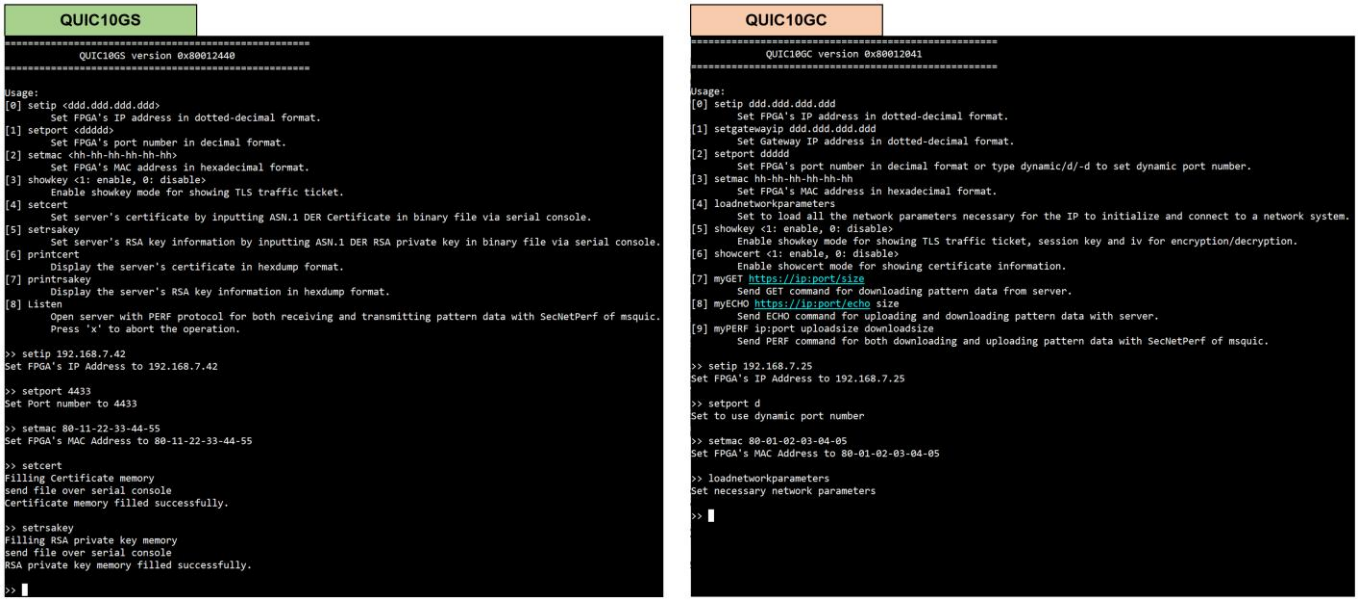

Figure 26 Server and client console display with configured parameters

7.2.2 Client download data test

command> myPERF <serverIP>:<serverPort> 0 <downloadSize>

Enter the command through the client's console, the client sends a request to download data from the server. The server responds by transmitting a data pattern of the specified size. Once the transfer is complete, both the client and server consoles display the transfer results and speed, as shown in Figure 27.

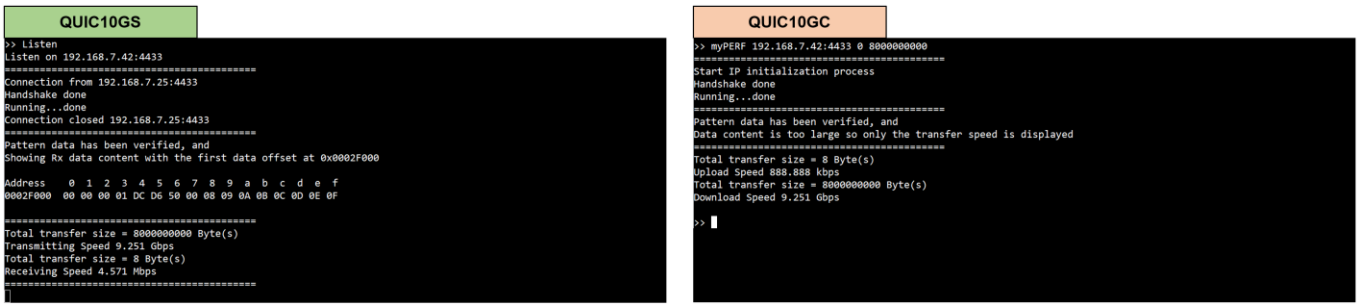

Figure 27 Server and client console display during data transfer from server to client

7.2.3 Client upload data test

command> myPERF <serverIP>:<serverPort> <uploadSize> 0

Enter the command through the client's console, the client generates and transmits a data pattern to the server. The server receives and processes the incoming data. Once the transfer is complete, both the client and server consoles display the transfer results and speed, as shown in Figure 28.

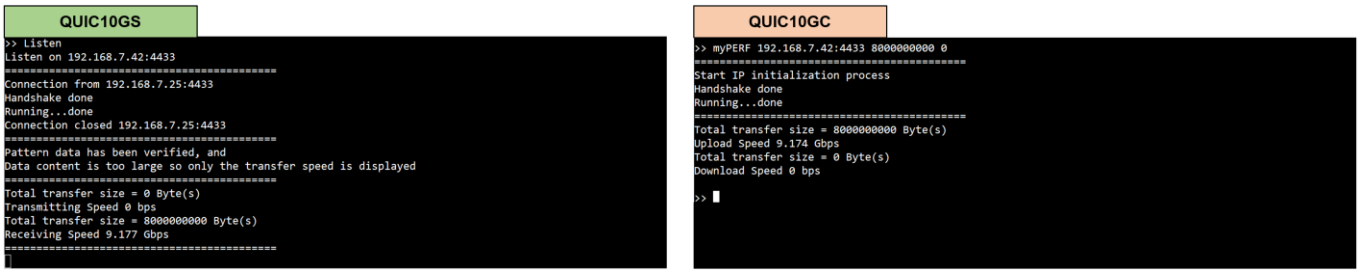

Figure 28 Server and client console display during data transfer from client to server

7.2.4 Client download/upload data test (Full duplex)

command> myPERF <serverIP:<serverPort> <uploadSize> <downloadSize>

Enter the command through the client's console, the client simultaneously sends an upload data pattern and requests a download data pattern from the server. The server responds by transmitting the requested data while receiving the client's data. Once the transfer is complete, both consoles display the transfer results and speed, as shown in Figure 29.

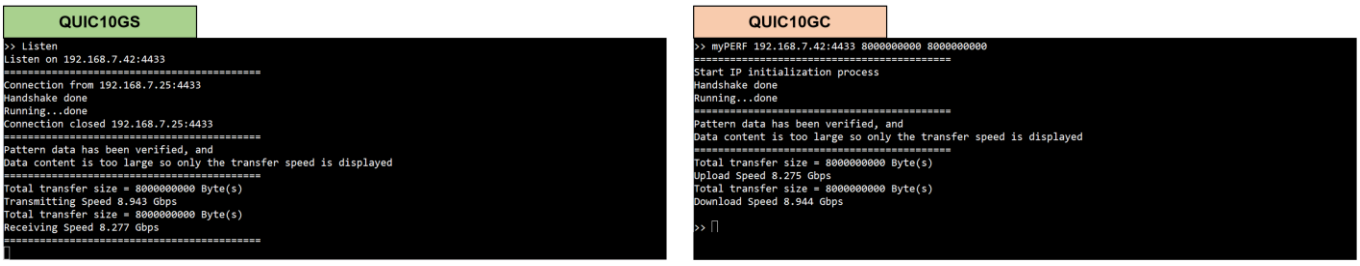

Figure 29 Server and client console display during Full-Duplex data transfer

8 Test Result

The performance test for QUIC10GS-IP on an FPGA board was conducted using QUIC10GS-IP as the QUIC server. At the application layer, a dedicated protocol—similar to MsQuic's 'secnetperf' example—was implemented to measure performance. The results compare the performance of QUIC10GS-IP with MsQuic's software as a client on a PC and QUIC10GS-IP with QUIC10GC-IP as a client on an FPGA.

When MsQuic, a software-based QUIC client running on a PC, downloads data from QUIC10GS-IP, the throughput is approximately 3.5 Gbps, while the upload speed reaches 8.7 Gbps. In the case of simultaneous upload and download, the throughput is around 2.5 Gbps. The utilization of the Intel i7 CPU is approximately 100%, as monitored by the PC's task manager. This indicates that the CPU is fully utilized when handling QUIC data transfer over the network.

On the other hand, when using QUIC10GC-IP as a client, the download speed from QUIC10GS-IP is approximately 9.2 Gbps, the upload speed is also 9.2 Gbps, and in the case of simultaneous upload and download, the throughput reaches 8.3 Gbps, as shown in Table 1.

Table 1 QUIC10GS-IP Performance test result

Client	Download (Gbps)	Upload (Gbps)	Full Duplex (Gbps)	CPU Utilization
MsQuic (Software on PC)	3.5	8.7	2.5	~100%
QUIC10GC-IP (on FPGA)	9.2	9.2	8.3	-

9 Revision History

Revision	Date (D-M-Y)	Description
1.00	12-Mar-25	Initial version release

