

# **QUIC10GS-IP Demo Instruction**

Env	ironmen	t Setup	3
PC	Setup		4
2.1	IP setti	ng	4
2.2	Speed	and duplex settings	5
2.3	Netwo	k properties settings	6
MsC	Quic serv	/er	9
FPC	GA deve	opment board setup	10
Seri	ial Cons	ble	11
Con	nmand c	letail	12
6.1	Set FP	GA's IP Address	12
6.2	Set FP	GA's Port Number	12
6.3	Set FP	GA's MAC address	12
6.4	Enable	showkey mode	13
6.5	Set ce	tificate	14
6.6	Set RS	A key information	15
6.7	Print c	ertificate	17
6.8	Print R	SA key information	18
6.9	Start a	server	19
Test	t setup v	/hen using 2 FPGA boards	21
7.1	Enviro	nment setup when using 2 FPGA boards	21
7.2	Test se	quence	22
	7.2.1	Set parameters and start a server	22
	7.2.2	Client download data test	22
	7.2.3	Client upload data test	23
	7.2.4	Client download/upload data test (Full duplex)	23
Test	t Result		24
Rev	ision His	story	25
	Env PC 2.1 2.2 2.3 Ms( FPC Seri 6.1 6.2 6.3 6.4 6.5 6.4 6.5 6.6 6.7 6.8 6.7 7.1 7.2 Tesi Rev	Environmen PC Setup 2.1 IP setti 2.2 Speed 2.3 Networ MsQuic serv FPGA devel Serial Conso Command d 6.1 Set FP 6.2 Set FP 6.3 Set FP 6.4 Enable 6.5 Set cer 6.6 Set RS 6.7 Print ce 6.8 Print R 6.9 Start a Test setup w 7.1 Enviror 7.2 Test se 7.2.1 7.2.2 7.2.3 7.2.4 Test Result .	Environment Setup PC Setup



# 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 <u>www.design-gateway.com</u>).



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

Ethernet 8 Properties	×	Internet Protocol Version 4 (TCP)	/IPv4) Properties	
etworking Sharing		General		
Connect using: 10-Gb LAN The Intel(R) Ethemet Controller X710 for 10Gb	E SFP+	You can get IP settings assigned this capability. Otherwise, you n for the appropriate IP settings.	d automatically if your network support need to ask your network administrator	s
	Configure	O Obtain an IP address autor	natically	
his connection uses the following items:		Use the following IP addres	ss:	
Client for Microsoft Networks	^	IP address:	192 . 168 . 7 . 25	
<ul> <li>The and Printer Sharing for Microsoft New — Nocap Packet Driver (NPCAP)     </li> </ul>	etworks	Subnet mask:	255 . 255 . 255 . 0	
QoS Packet Scheduler  Guide Content Protocol Version 4 (TCP/IPv4)	2	 Default gateway:		
Microsoft Network Adapter Multiplexor     Microsoft LLDP Protocol Driver	Protocol	Obtain DNS server address	automatically	
<	>	Use the following DNS serv	er addresses:	
Install	Properties	Preferred DNS server:		
Description		Alternate DNS server:		
Transmission Control Protocol/Internet Protoco wide area network protocol that provides corr across diverse interconnected networks.	ol. The default munication	Validate settings upon exit	Ad <u>v</u> anced	
		-	OK Com	

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.

Intel(R) E	thernet Con	troller X	710 for 1	0GbE SF	P+ Propertie	s	×
General	Advanced	Driver	Details	Events	Power Mana	agement	
The foll the prop on the r Property	owing propert berty you wan ight. /:	ties are a t to chan	vailable fo ge on the	orthis nei e left, and Va	twork adapter. I then select it alue:	. Click s value	_
Enable Energy Flow C Internu IPv4 C Jumbo Large 1 Link S Locally Log Lir Maximu Maximu	PME Efficient Eth ontrol to Moderation hecksum Offi Packet Send Offload Send Offload Send Offload Send Offload ate on Interfa Administered ik State Ever im Number of im Number of	ernet Nate load V2 (IPv4 V2 (IPv6 ace Dowr d Address nt f RSS Pro f RSS Qu			Disabled Disabled Enabled		
				E	ОК	Can	cel

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.

Intel(R) E	thernet Con	troller X	710 for 1	OGbE S	SFP+ Propert	ies	×
General	Advanced	Driver	Details	Event	s Power Mar	nagement	
The foll the prop on the r Property Flow C Interry Interry IPv4 C Jumbo Large Large Large Large Large Unk Si Locally Log Lir Maxim	owing propert perty you wan ight. y: PME PEfficient Eth control pt Moderation hecksum Offl Packet Send Offload Send Offload Send Offload tate on Interfar Administered nk State Ever um Number of um Number of	emet Rate oad V2 (IPv4 V2 (IPv6 sce Dowr I Address t RSS Pr f RSS Qu	vailable f ige on the ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) )	or this n	etwork adapte nd then select Value: 9014 Bytes 4088 Bytes 9014 Bytes Disabled	er. Click its value	
					OK	Car	ncel





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

Intel(R) Et	thernet Con	troller X	710 for 1	OGbE SFI	P+ Propertie	s	×
General	Advanced	Driver	Details	Events	Power Mana	agement	
The foll the prop on the r	owing propert berty you wan ight.	ies are a t to chan	vailable fo ge on the	orthisnet eleft, and	work adapter. then select it:	Click s value	
Property	r:			Va	lue:		
Link St Locally Log Lir Maximu Maximu Packet Prefem	ate on Interfa Administered nk State Ever um Number of um Number of t Priority & VL ed NUMA no	ace Down IAddress nt FRSS Pro FRSS Qu AN de			096		•
Receiv	e Buffers						
Receiv RSS B RSS lo Speed TCP CI TCP CI	re Side Scalir ase Processo ad balancing & Duplex hecksum Offl hecksum Offl	ng profile oad (IPv4 oad (IPv4	r 4) 5) V				
					ОК	Can	icel

#### **Figure 7 Receive Buffers**

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

Intel(R) E	thernet Con	troller X	710 for 1	OGbE SFI	P+ Propertie	25	×
General	Advanced	Driver	Details	Events	Power Mana	agement	
The foll the prop on the r	owing propert perty you wan ight.	ies are a t to char	vailable fo	orthis net e left, and	work adapter then select it	. Click s value	
Propert	y:			Va	lue:		
Maxim Packe Prefem Receiv RSS B RSS Is Speed TCP C TCP C TCP C UDP C VLAN	um Number of t Priority & VL ed NUMA no- ve Buffers ve Side Scalir lase Processo ad balancing & Duplex hecksum Offi hecksum Offi hecksum Offi hecksum Offi D	f RSS Qu AN de or Numbe profile oad (IPv oad (IPv load (IPv	4) 6) 4)		096		
					OK	Can	cel

Figure 8 Transmit buffers

### 3 MsQuic server

QUIC software implementation used in our reference is MsQuic, developed by Microsoft. Their work is an opensource software project, written in C and published in the following website: <u>github.com/microsoft/msquic</u>. 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: <u>github.com/design-gateway/msquic</u>. 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.

Vivado 2021.1	
ile Flow Iools Window Help Q. Quick Access	ii) Open target -> Auto Conr
	Hardware     Ø     Auto Connect       Q     ₹     ♦     Ø       Naviable Targets on Server >     Available Targets on Server >
Quick Start	HARDWARE MANAGER - localhost/xilinx_tcf/Digilent/210308AB9D59
Create Project >	Hardware ? X MIG - MIG_1
Open Project >	
Open Example Project > Tasks Manage IP > i) Click open Hardware Manager i	Name       Status         ✓ Il localibot (1)       iii) Select FPGA device to program bit file         ✓ Il vitins_tch( iii) Zrussk upen       Verify Zrussk upen         ✓ Il vitins_tch( iii) Zrussk upen       Verify Zrussk upen         ✓ Il vitins_tch( iii) Zrussk upen       Verify Device         Il vitins_tch( iii) Zrussk upen       Verify Device         Il vitins_tch( iii) Zrussk upen       Verify Device         Il viting Device       Verify Device         If Program Device       iv) Click Program device
Vivado Store >	Select a bitstream programming file and download it to your hardware device. You can optionally select a debug probes file that corresponds to the debug cores contained in the bitstream programming file.
Learning Center Documentation and Tutorials > Quick Take Videos > What's New in 2021.1 >	Bitstream file: 1/116/download/QUIC10GSTest.bit

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

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.



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.







### 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	>ope	ense	s1 )	x509	) —j	in c	ert	t. pe	em -	-ou	t ce	ert.	bir	n -0	outf	form	der   hexdump -C cert.der
000000	30	82	03	53	30	82	02	3b	a0	03	02	01	02	02	14	50	0S0;P
000010	10	dd	$\mathbf{bc}$	f4	a8	3c	<b>39</b>	69	76	11	<b>e</b> 8	b2	a0	$\mathbf{ca}$	2b	c5	+.
000020	67	89	8a	30	<b>0</b> d	06	09	2a	86	48	86	f7	<b>0</b> d	01	01	0b	g 0 *. H
000030	05	00	30	<b>38</b>	31	<b>0</b> b	30	09	06	03	55	04	06	13	02	54	081.0UT
000040	48	31	10	30	<b>0</b> e	06	03	55	04	08	<b>0</b> c	07	42	61	6e	67	H1.0UBang
000050	6b	6f	6b	31	17	30	15	06	03	55	04	0a	<b>0</b> c	<b>0</b> e	44	65	kok1.0UDe
000060	73	69	67	6e	20	47	61	74	65	77	61	79	30	20	17	0d	sign GatewayO
000070	<b>32</b>	33	30	32	32	<b>34</b>	30	39	<b>32</b>	38	31	30	5a	18	0f	32	23022409281072
000080	31	32	33	30	31	33	31	30	<b>39</b>	32	38	31	30	5a	30	<b>38</b>	1230131092810Z08
000090	<b>31</b>	0b	30	09	06	03	55	04	06	13	02	54	48	31	10	30	1. 0 U TH1. 0
0000a0	<b>0</b> e	06	03	55	04	08	<b>0</b> c	07	42	61	6e	67	6b	6f	6b	31	UBangkok1
0000b0	17	30	15	06	03	55	04	0a	0c	0e	44	65	73	69	67	6e	.OUDesign
0000c0	20	47	61	74	65	77	61	79	30	82	01	22	30	0d	06	09	GatewayO"O
0000d0	2a	86	48	86	f7	<b>0</b> d	01	01	01	05	00	03	82	01	0f	00	*. H
0000e0	30	82	01	0a	02	82	01	01	00	$\mathbf{c0}$	36	8c	0a	dc	4f	bf	060.
0000f0	<b>0</b> b	1c	40	3c	77	17	$\mathbf{ef}$	bb	81	$\mathbf{f3}$	c5	02	d2	f7	$\mathbf{ca}$	ca	@ <w< td=""></w<>
000100	96	$\mathbf{ca}$	d0	$\mathbf{cd}$	3f	0b	48	$\mathbf{c1}$	87	$\mathbf{fc}$	f3	b7	13	5e	<b>29</b>	b6	?.H^).
000110	c9	96	19	f4	$\mathbf{ed}$	$\mathbf{bc}$	c2	8d	$\mathbf{eb}$	af	$\mathbf{f6}$	92	0a	a2	b9	93	
000120	5c	$\mathbf{cf}$	<b>34</b>	bd	1b	3c	<b>d</b> 1	<b>24</b>	54	7f	<b>59</b>	6b	75	9f	f7	00	\. 4 <. \$T. Yku
000130	ee	38	4a	13	60	72	96	<b>23</b>	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. +\$0. d6 U
000150	df	<b>8f</b>	03	07	2e	eb	97	e8	64	78	73	17	18	a4	7b	79	dxs {y
000160	2a	$\mathbf{f}\mathbf{b}$	5e	4d	75	06	$\mathbf{c4}$	43	62	ba	$\mathbf{c7}$	5f	a9	72	e5	8e	*. MuCbr
000170	74	c5	ae	b5	fe	98	65	49	d3	7f	$c_0$	de	39	$\frac{31}{2}$	9d	06	t
000180	38	ac	fa	ad	68	64	d0	3a	b9	51	d6	24	53	$\frac{7c}{7c}$	81	67	8hd.:.Q. \$S .g
000190	fd	db	19	a9	a8	95	34	00	7e	83	fl	68	6c	59	ca	49	4hIY.I
0001a0	ld	99	d7	34	4c	56	01	Za	83	dI	5C	12	cb	<u>c8</u>	83	4b	$\dots 4LV. \star \dots h$
0001b0	aa	53	58	11	eb	33	CU	bd	aZ	89	le	4e	59	75	91	54	. SX 3 NYU. I
001100	(8 -1-	90	85	3C		60	12	69			91	е1 ⊾о	95	aa	25	dZ	$\mathbf{X}$ $(\mathbf{r}$ ] $(\mathbf{N}$ .
000100	CD	eo JE	90	a1 09	00 47	40 JL	34 75	29 0f	10	00	01	D3 01	80	aa 01	CC	29 50	$ 5 \Pi 4 / j . 0 )$
000160	ao 20	00 51	30	04	41	an	10	11	91	02	16	01	14	40	aə 97	00	
000110	30	10	30	10 75	00	00	50 E0	10	Ue 6 a	19	10	04 74	14	da	21	4C J£	
000200	41	24	40	10	02	uo	00 1 J	00		10	ec	16	19	0e	11	01 97	
000210	ae 1	<i>J</i> 1	11 91	45	00 7h	00 09		20 58	04 0h	10	12	10	71	14 f0	ua 60	ム1 千千	$1 \wedge e_{F} / V + P$
000220	40 4f	41	24	40 0f	66	02	40 55	1d	12	00	13 01	ec ff	04	15	30	U3 TT	
000230	01	αe Λ1	50 ff	30	60	05	00	1u 9a	86	18	86	f7	604	01	01	05 0b	0 * H
000240	05	00	03	82	01	01	00	2a 2d	60	31 21	35	25	85	hR	81	00	= 155
000230	61	20 20	25	c0	47	98 98	56	AC	23 23	93 93	00	13	28	50		2c	a % C V (P
000200	32	35	$\hat{0}\mathbf{f}$	22	c5	a0 a0	32	42	74	4d	54	28	28	6a	c8	d7	$25 \ 3 \ 9\text{R+MT}((i)$
000210	4c	h2	80	00	90	d0	a9	5h	06	-6	60	$14^{-20}$	25	91	18	ed	
000290	<u>р</u> 1	ef	31	42	10	86	72	$f^2$	4d	1h	60	$14^{11}$	$\hat{0}_{\mathbf{C}}$	6f	$\hat{0}_{\mathbf{C}}$	96	1B r M o
0002a0	de	ff	dÂ	9e	85	d6	89	7e	49	a8	59	6a	8a	$\tilde{21}$	28	f7	
0002b0	36	15	10	e7	11	e3	78	48	4c	$a^2$	30	bf	b4	93	f0	38	6xHL. 08
0002c0	27	<u>9</u> 9	ce	d1	73	de	42	fc	$\tilde{02}$	25	3c	f2	1f	bd	aa	32	's. B%<2
0002d0	02	2f	eb	21	cb	78	$\mathbf{c}0$	cf	$c^2$	ee	84	e9	bf	eb	35	ab	/. !. x
0002e0	f4	c8	71	6c	23	e8	f5	61	e6	03	8c	2d	43	1c	0a	bf	ql#aC
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	<b>0</b> b	d4	30	eb	y.@W0.
000320	2a	29	ae	f6	70	b2	f4	a3	61	5d	b8	6c	e0	$\mathbf{cd}$	fb	51	*)pa].1Q
000330	96	7a	01	18	12	1c	3f	76	c4	84	d2	a8	9e	6f	65	fb	. z?voe.
000340	07	29	d9	<b>24</b>	<b>c</b> 0	$\mathbf{f}\mathbf{d}$	10	e4	98	3a	b3	$\mathbf{ab}$	b4	76	4d	c0	.).\$vM.
000350	de	44	00	4e	e1	$\overline{37}$	62										. D. N. 7b

Figure 16 Certificate information from openssl command



#### QUIC10GS IP Core

M4 - Tera Term VT		
le cdit <u>S</u> etup C <u>o</u> ntrol	Window	Help
New connection	Alt+N	
Duplicate session	Alt+D	
Cygwin connection	Alt+G	
Log		
Pause Logging		
Comment to Log		idd>
View Log		dress in dotted-decimal format.
Show Log dialog		In the second se
Stop Logging (O)		2 bbb
Send file		dress in hexadec:
Iranster	>	0: disable>
SSH SCP		node for showing TI 🔤 😽 🔤 🥵
Peplay Log		cert.der key.der
Replay Log		tificate by input serial console.
TTY Record		key information k
П керіау		
Print	Alt+P	ver's certificate :
Disconnect	Alt+I	Files of type: All(**) Cancel
Exit	Alt+Q	ver's RSA key info
Exit All		
Open serv	ver wit	with SecNetPerf of msquic.
Press x	to at	port the operation.
> setcert		
illing Certifica	ate men	tory
end file over se	erial c	console

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>	ope	enss	:1 r	·sa	-ir	ı ke	ey.r	oem	-οι	ıt k	key.	der	· -c	outf	orm	der	•	hexdump -	-C key.	deı
writing	RSA	ke	ey -				- <b>J</b> - <b>F</b>				) -								j-	
$000000^{-}$	30	82	04	be	02	01	00	30	<b>0</b> d	06	09	2a	86	48	86	f7	0		*.H	
000010	0d	01	01	01	05	00	04	82	04	a8	30	82	04	a4	02	01		0.	••••	
000020	00	02	82	01	01	00	c0	36	8c	0a	dc	4f	$\mathbf{bf}$	0b	1c	40		6	)@	
000030	3c	77	17	ef	bb	81	$f_{3}$	cb	02	d2	17	ca	ca	96	ca	d0	<w.< td=""><td></td><td>••••</td><td></td></w.<>		••••	
000040	Cd ⊈₄	31	00	48		87	1C	13 £6	b7	13	5e	29	bb	c9	96 -f	19	. ?.	н,	)	
000050	14 64	ea 1h	bc 2	CZ	80 94	eb 54	ar 7f		92 61	$\frac{0a}{75}$	az of	b9 £7	93	5C	00 00	34 4 a	••• /	•••••••••••••••••••••••••••••••••••••	••\•4	
000000	มน 1 จ	60	3C 79	96	24 99	04	11 91	09 6h	00	70	91 99	10	Q1	69 63	00 8f	4a 9h	$\cdot$	. фі. ікц • # 11- 7"(	0 c +	
000010	24	4f	07	64	36	d7	af	55	14	h8	98	eh	f7	df	8f	03	\$0 <sup>1</sup>	d6 II	s. C. '	
000090	07	$\frac{11}{2e}$	eb	97	e8	64	78	73	17	18	a4	7b	79	$\frac{1}{2a}$	fb	5e	φΟ.	dxs	{v*. ^	
0000a0	4d	75	06	c4	43	62	ba	c7	$\hat{5}\mathbf{f}$	a9	$\overline{72}$	e5	8e	74	c5	ae	Mu.	.Cbr.	.t	
0000b0	b5	fe	98	65	49	d3	7f	$\mathbf{c0}$	de	39	31	9d	06	38	ac	fa		eI91.	. 8	
0000c0	ad	68	64	d0	3a	b9	51	d6	<b>24</b>	<b>53</b>	7c	81	67	$\mathbf{fd}$	db	19	.hd	l. : . Q. \$S .	g	
0000d0	a9	a8	95	34	00	7e	83	$f_1$	68	6c	59	ca	49	$1 \mathrm{d}$	99	d7	• • •	4. ~. h1Y.	I	
0000e0	34	4c	56	01	2a	83	d1	5c	12	cb	<u>c8</u>	83	4b	aa	53	58	4LV	. * \	K. SX	
000010	11	eb fb	33	c0	bd	a2	89 J1	1e 07	4e	59	75	91	54 19	78	9d	85	3	NYu.	. Tx	
000100	3C			12	09	11 74	ն1 հջ	91 6f	e1 62	90	aa	20	0Z	CD	eo 45	90	< CU	$r_1, \ldots, r_n$	<sup>%</sup>	
000110	a1 89	00 17	40 dh	04 75	29 8f	0f	00	01	03	00	aa 01	02	29 89	ao 01	00	90 97	. Sn	l4)∫. 0 11		
000120	$c_6$	$\hat{0}\mathbf{f}$	ad	9a	6f	a7	48	47	$\hat{0}\mathbf{f}$	09	17	37	6d	10	d3	4e		. o. HG '	7m N	
000140	b1	$1\overline{1}$	0e	1a	$\tilde{92}$	81	92	$\hat{4}d$	74	52	1c	7c	5c	$\overline{74}$	32	$\hat{25}$		MtR.	\t2%	
000150	4c	08	c2	<b>24</b>	$\mathbf{f}\mathbf{f}$	7c	17	1f	96	$\mathbf{c8}$	$\mathbf{dc}$	40	$\mathbf{c2}$	78	37	b3	L	\$.   (	Ø. x7.	
000160	6c	dd	b4	88	<b>b</b> 1	f6	e4	f8	37	4f	$\mathbf{fd}$	87	8b	2a	c2	b0	1		.*	
000170	9d	23	d9	1c	22	1f	67	9b	a2	10	61	3c	88	82	ab	3f	. #.	". g a	</td <td></td>	
000180	fb	12	94	5b	<u>69</u>	d3	ac	ad	f0	91	31	$\mathbf{fc}$	c9	al	c1	d5	••••	Li1.		
000190	70	46	81	fb	70	de	53	af	e4	01	b6	eb	c5	fe	42	c6	pF.	. p. S	B.	
0001a0 0001b0	eð	69	8C	a5 20	00		00		al	a4 24	8Z 94	84 55	T d	UZ 54	Za	bc G	.1.		· · · *.	
000100	აა 6f	00	0Z 1A	১৮ ২1	20	22	ა <u>კ</u>	2C 62	aa 10	54	24 01	00 47	19	00 19	94 oh	oe nn	ວ. ມ ດ	19, 2,a 16 bat	L• ]• II R	
000100 0001d0	75	80	76	ha	20	$\frac{2}{2}$ d	80	$f_3^{02}$	65	34	3c	67	ec	hf	42	27	11 V	- e4<	σ R'	
0001e0	da	2f	36	d3	7c	56	2f	38	d8	fd	a4	6a	c8	87	7e	ae	. /6	.  V/8	i	
0001f0	09	6a	74	$\mathbf{a4}$	05	38	74	12	37	27	<b>26</b>	$\mathbf{c4}$	de	<b>35</b>	0e	3b	.jt	8t.7'&	. 5. ;	
000200	b1	<b>c</b> 8	75	e6	c1	17	55	f1	10	4d	$\mathbf{fd}$	48	5a	$\mathbf{a0}$	73	eb	u	UM. I	IZ. s.	
000210	93	d3	0d	81	3e	ad	00	92	a2	9f	31	$\frac{3f}{5}$	ad	c9	43	7a		$\cdot \cdot \cdot \cdot \cdot \cdot 1$	?Cz	
000220	af	d7	70	ba	07	5e	cb	7d	c8	db	33	5b	bc	13	91	02	•• p	··· · } · · 3	L	
000230	81	81 79	00	el	b3		C9	71 59	98	0b	2b	75 fb	bb	11	9c	bd		q+1	1	
000240 000250	22 56	19	09 25	3C 46	22 57	$\frac{\partial \mathbf{I}}{\partial \mathbf{f}}$	90 88	บอ ล4	eu a5	oc 5a	1e 4f	1D f0	a1 10	อต 93	a0 13	eo fN	vs.	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	· · ∖• • ⊺#	
000250	97	$\frac{12}{32}$	ao 8c	-10 c6	66	$f^{1}$	c9	h4	a5 82	Ja 1a	f7	f0	49 aa	$h^{20}$	d5	c0	2	f	1	
000270	e8	50	67	87	bb	2f	a2	cc	58	51	cb	d1	45	46	91	82	.Pg	/XQ.	EF.	
000280	43	00	dc	b1	4d	f5	b4	c6	da	8a	96	65	bb	d5	e6	52	С	. M	eR	
000290	ee	60	35	<b>24</b>	$\mathbf{fa}$	94	db	13	39	7c	96	46	6a	99	9b	ea	• 5	i\$9 .1	Fj	
0002a0	3f	50	d0	83	2c	25	71	de	9d	$c_2$	fb	8c	d0	0c	c4	f9	?Р.	.,%q		
0002b0	08	58	29	02	81	81	00	da	03	d7	3f	2a	62	dd	05	85	.X)	~ [1	*b	
000200	(D	e /	() 22	d9 10	00	80 77	82	7e	35 24	(b) 1f	31 55	9e	25	3e 97	a5 2f	00 46	ر. u	5 - 5 = - 5	.%∕.⊥ _'9	
000200 000200		a4	აა 51	19 5h	90 0f	26	uu 2f	ce h1	əu Sh	11	٥D م1	Zu Af	44 43	21	$\frac{\partial I}{\partial A}$	uo 19		)w[*	$-$ . $\cdot$ .	
0002c0	h3	93	55	ef	$04^{-1}$	$c_5$	$\frac{21}{31}$	81	15	c8	5f	8c	h6	64	94	e5	· · •	1	d 12.0	
000300	b7	a3	29	52	e1	30	7c	ef	ae	07	63	76	06	96	54	2d	)	$\mathbf{R}$ . $0$ $1$ $$ $\mathbf{c}$	vT-	
000310	be	7e	6e	92	02	52	ea	e7	46	80	6c	e6	8a	<b>35</b>	e8	7a	.~'n	R. F. 1.	.5.z	
000320	e8	dd	d7	80	9d	7c	4a	87	6f	e8	00	80	c2	<b>57</b>	79	42		J. o	.WyB	
000330	e3	4e	fa	33	40	$c^2$	87	02	81	81	00	9c	91	df	7b	0b	. N.	3@	· • • {•	
000340	el L	14	86	8e	82	3a	02	88 95	35	d8	fe	21	88	02	17				/	
000350	04 10	9a	eo dd	00 5d	04 6h	C1	00 f8	or SP	04 99	00	14 ff	30	2a 26	11 f6	00 5f	44 h/			. ^. SU \6	
000300	67	h8	fh	9c	a9	5d	ah	e8	<u>c</u> 9	7f	$\frac{11}{d5}$	82	13	f9	44	o <del>r</del> af	• ,• σ	]	/0. <u>.</u> .	
000380	0a	e9	9b	41	4e	14	59	26	8b	$\dot{02}$	93	16	30	65	ad	85		AN. Y&	0e	
000390	70	df	48	db	$\mathbf{c4}$	04	eb	65	46	55	d9	28	10	e8	a8	5c	<b>p.</b> H	leFU.	()	
0003a0	da	b9	<b>31</b>	aa	<b>21</b>	92	f3	d4	f9	1  d	3f	b8	$\mathbf{6f}$	2c	7e	a4	1	. !?.	0,~.	
0003b0	96	be	47	30	74	b7	17	01	46	a7	99	02	81	81	00	97	G	0tF	••••	
0003c0	74	03	9c	45	fd	d8	3d	75	b5	d5	dd	f0	9a	84	d7	32	t	E =u	2	
0003d0	80	44 £0	с <b>р</b>	1b oc	be	34 42	41	07	ba	$\frac{1}{7}$	41 94	CZ	7a Ga	b1 99	ba df	4d 7 o	. D.	. n40. j. 0.	$Z \cdot M$	
000360 0003£0	00 08		DC FQ	00 57	er	uə ff	42 05	43 00	1e 20		2u	20 10	00	ა <u>კ</u>	ui 5h	7e 61		DII. – o W	хшZ. Г	
000310	ео а9	38	<u>1</u> 41	e8	сс а6	ec	c8	e3	ac	эс е7	14	56	17	ua 4a	70	00	. м. 8А	"	V.In	
000410	b1	8d	40	73	45	b0	39	5a	6d	f3	b7	2c	87	a0	c2	bf	@	sE. 9Zm		
000420	58	22	ef	84	58	8f	8a	a9	98	0c	45	21	7c	46	54	20	Х".	. X E	!   FT	
000430	32	85	a1	93	<b>d</b> 1	6e	a3	36	ec	62	79	3e	11	c7	11	02	2		>	
000440	81	80	6c	0f	eb	d1	9c	88	99	3f	b4	94	bf	4b	73	00	$\cdot$ 1	?	.Ks.	
000450	be	a7	71	9b	da	cc	50	bl	48	9f	78	47	c4	77	c4	16	. q	P. H. x	j. W	
000460	21 20	34	$\frac{01}{fc}$	1C	0a	$\frac{04}{29}$	34 51	20 fr	b5 70	1a 79	1C 60	9a	91 ba	74 f0	75 0E		$\overline{0}^{4}$	14	.tu.	
000470	59 13	ac a4	$\frac{10}{72}$	01 31	10	32	od	10	79 da	72 8b	09	22 h4	ba c0	19 79	00 45	5е f3	9	$\cdot \cdot 2 ] \cdot yr1$	····>	
000490	10 55		df	69 69	17	df	$\frac{1}{2c}$	eh	ua 89	70	ое а3	h6	fh.	67	96	fa	II.	n	σ	
0004a0	dc	cd	44	78	5e	80	47	e9	36	3c	c3	d3	21	78	35	2d	D	x^. G. 6<	!x5-	
0004b0	ed	9d	9d	97	ee	3c	cd	b1	93	b4	59	47	5d	0b	c6	12		<y< td=""><td>G]</td><td></td></y<>	G]	
0004c0	a5	b4																		

#### Figure 18 RSA key information from openssI 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.

>> printc	ert																
Certifica	te i	info	orma	atio	on												
0000000	30	82	03	53	30	82	02	3B	A0	03	02	01	02	02	14	50	0S0;P
00000010	10	DD	BC	F4	<b>A</b> 8	3C	39	69	76	11	E8	B2	A0	CA	2B	C5	<9iv+.
00000020	67	89	<b>8</b> A	30	0D	06	09	2A	86	48	86	F7	0D	01	01	0B	g0*.H
0000030	05	00	30	38	31	0B	30	09	06	03	55	04	06	13	02	54	081.0UT
00000040	48	31	10	30	0E	06	03	55	04	08	0C	07	42	61	6E	67	H1.0UBang
00000050	6B	6F	6B	31	17	30	15	06	03	55	04	ØA	0C	0E	44	65	kok1.0UDe
0000060	73	69	67	6E	20	47	61	74	65	77	61	79	30	20	17	0D	sign Gateway0
30000070	32	33	30	32	32	34	30	39	32	38	31	30	5A	18	ØF	32	23022409281072
0000080	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	1.0UTH1.0
900000A0	ØE	06	03	55	04	08	0C	07	42	61	6E	67	6B	6F	6B	31	UBangkok1
900000в0	17	30	15	06	03	55	04	ØA	0C	<b>0</b> E	44	65	73	69	67	6E	.0UDesign
900000C0	20	47	61	74	65	77	61	79	30	82	01	22	30	0D	06	09	Gateway0"0
300000D0	2A	86	48	86	F7	0D	01	01	01	05	00	03	82	01	0F	00	*.H
300000E0	30	82	01	0A	02	82	01	01	00	<b>C</b> Ø	36	8C	ØA	DC	4F	BF	060.
300000F0	ØB	1C	40	3C	77	17	EF	BB	81	F3	C5	02	D2	F7	CA	CA	@ <w< td=""></w<>
0000100	96	CA	D0	CD	3F	0B	48	C1	87	FC	F3	Β7	13	5E	29	B6	^).
00000110	C9	96	19	F4	ED	BC	C2	8D	EB	AF	F6	92	0A	A2	B9	93	
0000120	5C	CF	34	BD	1B	3C	D1	24	54	7F	59	6B	75	9F	F7	00	
0000130	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.+\$0.d6U
00000150	DF	8F	03	07	2E	EB	97	E8	64	78	73	17	18	A4	7B	79	dxs{v
0000160	2A	FB	5E	4D	75	06	C4	43	62	BA	C7	5F	A9	72	E5	8E	*.^MuCbr
00000170	74	C5	AE	B5	FE	98	65	49	D3	7F	C0	DE	39	31	9D	06	teI91
0000180	38	AC	FA	AD	68	64	D0	3A	B9	51	D6	24	53	7C	81	67	8hd.:.0.\$S .g
00000190	FD	DB	19	A9	<b>A</b> 8	95	34	00	7E	83	F1	68	6C	59	CA	49	14.~hlY.I
000001A0	1D	99	D7	34	4C	56	01	2A	83	D1	5C	12	СВ	C8	83	4B	4LV.*\K
000001B0	AA	53	58	11	E6	33	C0	BD	A2	89	1E	4E	59	75	91	54	.SX3NYu.T
00001C0	78	9D	85	3C	FB	<b>C8</b>	72	69	1F	D1	97	E1	95	AA	25	D2	x <ri%.< td=""></ri%.<>
000001D0	CB	E8	90	A1	53	48	34	29	7D	B8	6F	<b>B</b> 3	80	AA	СС	29	SH4)}.o)
000001E0	<b>A8</b>	D5	9C	82	47	DB	75	8F	9F	02	03	01	00	01	A3	53	Ś
000001F0	30	51	30	1D	06	03	55	1D	0E	04	16	04	14	DA	27	4C	000U'L
30000200	41	24	45	7B	02	D8	58	0B	6C	13	EC	74	F9	6E	FF	DF	A\$E{X.lt.n
0000210	AE	30	1F	06	03	55	1D	23	04	18	30	16	80	14	DA	27	.0U.#0'
0000220	4C	41	24	45	7B	02	D8	58	0B	6C	13	EC	74	F9	6E	FF	LA\$E{X.lt.n.
0000230	DF	AE	30	ØF	06	03	55	1D	13	01	01	FF	04	05	30	03	
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	<b>B</b> 8	84	0D	=.155
00000260	61	A0	25	C0	47	<b>A8</b>	56	EC	A3	<b>A</b> 3	09	13	28	50	EE	2C	a.%.G.V(P.,
00000270	32	35	ØF	33	C5	A9	32	42	74	4D	54	28	28	6A	<b>C8</b>	D7	25.32BtMT((j
00000280	4C	B2	80	CC	90	D0	A9	5B	06	E6	60	14	25	91	18	ED	L[`.%
0000290	E1	EF	31	42	1E	86	72	F2	4D	1B	9D	14	0C	6F	0C	96	1Br.Mo
000002A0	DE	FF	D8	9E	85	D6	89	7E	49	<b>A8</b>	59	6A	<b>8</b> A	21	28	F7	
000002B0	36	15	10	E7	11	E3	78	48	4C	A2	30	BF	Β4	93	F0	38	6xHL.08
000002C0	27	99	CE	D1	73	DE	42	FC	02	25	3C	F2	1F	BD	AA	32	's.B%<2
300002D0	02	2F	EB	21	CB	78	C0	CF	C2	EE	84	E9	BF	EB	35	AB	./.!.x5.
300002E0	F4	<b>C8</b>	71	6C	23	<b>E8</b>	F5	61	E6	03	8C	2D	43	1C	ØA	BF	ql#aC
000002F0	E8	E1	99	E8	B2	93	A0	45	DA	58	15	ED	35	A2	ØA	A1	E.X5
0000300	E2	75	EE	EA	<b>C8</b>	<b>8</b> A	9F	B9	D0	46	D9	7A	76	44	FB	F1	.uF.zvD
00000310	FA	9B	AB	<b>A8</b>	79	DC	40	7F	15	8D	57	A7	0B	D4	30	EB	y.@W0.
0000320	2A	29	AE	F6	70	B2	F4	<b>A</b> 3	61	5D	<b>B8</b>	6C	E0	CD	FB	51	<pre>*)pa].10</pre>
00000330	96	7A	01	18	12	1C	3F	76	C4	84	D2	<b>A8</b>	9E	6F	65	FB	.z?voe.
00000340	07	29	D9	24	C0	FD	10	E4	98	3A	<b>B</b> 3	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

>> printrsakey

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.

RSA Key i	nfor	mat	io	n													
00000000	30	82	04	BE	02	01	00	30	ØD	06	09	2A	86	48	86	F7	00*.н
00000010	ØD	01	01	01	05	00	04	82	04	A8	30	82	04	A4	02	01	
000000020 00000030	3C	77	17	EF	BB	81	F3	36 C5	02	D2	F7	4F CA	CA	96	CA	40 D0	
00000040	CD	3F	ØB	48	C1	87	FC	F3	B7	13	5E	29	B6	C9	96	19	.?.H^)
00000050	F4	ED	BC	C2	8D	EB	AF	F6	92	ØA	A2	B9	93	5C	CF	34	
00000060	BD	1B	3C	D1	24	54	7F	59 6 P	6B	75	9F	F7	00	EE	38	4A	
00000070	24	4F	07	64	36	97 D7	AF	55	14	B8	98	EB	94 F7	DF	8F	03	\$0.d6U
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	MuCbrt
000000B0 000000B0	B5	FE	98	65 D0	49	D3 BO	7F	C0	DE	39	31	9D 91	Ø6	38	AC	FA 10	eI918
00000000000000000000000000000000000000	AD A9	A8	95	34	00	7E	83	F1	68	60	59	CA	49	1D	99	D7	14.~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	CØ	BD	A2	89	1E	4E	59	75	91	54	78	9D	85	
00000100	3C 41	FB	48	72	69 29		D1 B8	97 6F	E1 B3	95		25	D2 29	CB A8	E8	90	<r1%< td=""></r1%<>
00000120	82	47	DB	75	8F	9F	02	03	01	00	01	02	82	01	00	2D	.G.u
00000130	C6	ØF	AD	9A	6F	A7	48	47	ØF	09	17	37	6D	10	D3	4E	o.HG7mN
00000140	B1	11	ØE	1A	92	81	92	4D	74	52	10	7C	5C	74	32	25	MtR. \t2%
00000150 00000160	4C	08 DD	C2 B4	24 88	FF B1	F6	17 E4	IF F8	96 37	C8	DC FD	40	C2 8B	78 24	37	83 80	L\$. @.x7.  170*
00000170	9D	23	D9	10	22	1F	67	9B	A2	10	61	30	88	82	AB	3F	.#".ga </td
00000180	FB	12	94	5B	69	D3	AC	AD	FØ	91	31	FC	C9	A1	C1	D5	[i1
00000190	70	46	81	FB	70	DE	53	AF	E4	01	B6	EB	C5	FE	42	C6	pFp.SB.
000001A0 000001B0	E8	69 08	8C 62	A5 39	20	FD 22	32	FD 2C		A4 3D	82 24	84 5B	FD 19	02 5D	2A 94	BC 6E	.1*.  3.b9."2=\$[.]_n
00000100	6F	AA	14	31	36	E2	E2	62	40	54	04	D7	00	42	EB	00	o16b@TB
000001D0	75	80	76	BA	20	2D	80	F3	65	34	3C	67	EC	BF	42	27	u.ve4 <gb'< td=""></gb'<>
000001E0	DA	2F	36	D3	70	56	2F	38	D8	FD	A4	6A	C8	87	7E	AE	./6. V/8j~.
000001F0 00000200	09 B1	6A C8	74 75	A4	05 C1	38 17	74 55	12 F1	37	27 4D	26 FD	48	DE 54	35 40	0E 73	3B FB	.jt8t./ &5.;
00000210	93	D3	ØD	81	3E	AD	00	92	A2	9F	31	3F	AD	C9	43	7A	>1?Cz
00000220	AF	D7	70	BA	07	5E	СВ	7D	C8	DB	33	5B	BC	13	91	02	p^.}3[
00000230	81	81	00	E1	B3	DB	C9	71	98	ØB	2B	75	BB	11	90	BD	q+u
00000240 00000250	56	73	89 A5	3C 46	57	51 4E	5D 88	B3 A4	ED A5	8C 54	FE 4E	FØ	AF 49	23	A0	FØ	S.< Q]<  VFWO70.T#
00000260	97	32	80	C6	66	F2	C9	B4	82	1A	F7	FØ	AA	B2	D5	CØ	.2f
00000270	E8	50	67	87	BB	2F	A2	СС	58	51	CB	D1	45	46	91	82	.Pg/XQEF
00000280	43	00	DC	B1	4D	F5	B4	C6	DA	8A	96 06	65	BB	D5	E6	52	CMeR
00000290 000002A0	3E	50	35 DØ	83	FA 2C	25	71	DE	39 9D	C2	96 FB	46 8C	6A DØ	99	9B C4	EA F9	. 5\$9 .F]   ?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.%>.1
000002D0	AF	A4	33	19	90	77	0D	CE B1	3D	1F	5B	2D	D4	27	3F	D6	3w=.['?.
000002E0 000002E0	B3	93	51 55	EF	0F	56 C5	31	81	3B 15	C8	5F	4F 8C	43 B6	52 64	ге 94	42 E5	U1d
00000300	B7	A3	29	52	E1	30	7C	EF	AE	07	63	76	06	96	54	2D	)R.0 cvT-
00000310	BE	7E	6E	92	02	52	EA	E7	46	80	6C	E6	8A	35	E8	7A	.~nRF.15.z
00000320	E8	DD	D7	80	9D	70	4A	87	6F	E8	00	80	C2	57	79 78	42 08	J.oWyB
00000330	E3	4E	FA 86	33 8E	82	3A	02	88	35	81 D8	FE	9C	91 88	02	7В F7	C4	{. 
00000350	B4	9A	E5	DB	84	C1	C3	3F	B4	88	F4	BC	2A	1F	53	44	?*.SD
00000360	10	2C	DD	5D	6B	EE	F8	8B	22	E7	FF	ЗE	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.
00000390	0A 70	E9 DF	9B 48	41 DB	4E C4	14 04	EB	65	8B 46	55	93 D9	28	30 10	65 E8	AD	85 5C	p.HeFU.()
000003A0	DA	B9	31	AA	21	92	F3	D4	F9	1D	3F	B8	6F	20	7E	A4	1.!?.o,~.
000003B0	96	BE	47	30	74	B7	17	01	46	A7	99	02	81	81	00	97	
000003C0	74	03	90	45	FD	D8	3D	75	B5	D5	DD	FØ	9A	84 B1	D7	32	tE=u2
000003D0 000003F0	86	44 F8	C6 BC	FB 86	E1	54 D3	4F 42	6F	6A 1F	10 7E	4F 2D	26	7A 6D	B1 32	BA DE	4D 7E	Bn.~-&m2 ~
000003F0	E8	4D	F9	57	EE	FF	05	D3	AØ	90	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	.8AV.Jp.
00000410	B1	8D	40	73	45	BØ	39	5A	6D	F3	B7	2C	87	AØ	C2	BF	@sE.9Zm,
00000420 00000430	58	22 85	EF A1	84 93	58 D1	8F	8A A3	A9 36	98 EC	62	45 79	21 3E	7C	46 C7	54 11	20	A A E!   FT
00000440	81	80	60	ØF	EB	D1	90	88	99	3F	B4	94	BF	4B	73	00	1
00000450	5E	A7	71	9B	DA	СС	50	B1	48	9F	78	47	C4	77	C4	16	^.qP.H.xG.w
00000460	5F	34	ØF	7C	ØA	04	34	20	B5	FA	FC	9A	91	74	75	BA	_4. 4tu.
00000470 00000480	39	AC A4	F6	BF 31	F5 FA	32 FA	5D CE	43	79 DA	72 8B	69 0E	22 B4	BA	F9 72	85 D5	SE F3	92].yr1">
00000490	55	ØE	DF	E9	17	DF	20	EB	89	70	A3	B6	FB	67	96	FA	U,pg
000004A0	DC	CD	44	78	5E	80	47	E9	36	3C	С3	D3	21	78	35	2D	Dx^.G.6 x5-</td
000004B0	ED	9D	9D	97	EE	3C	CD	Β1	93	B4	59	47	5D	ØB	C6	12	YG]
STREET, STREET																	

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																	
Connectic Handshake Running	on fr dor .dor	rom ne ne	192	2.10	58.7	7.25	5:50	0293	3			=					
Connectio	on cl	lose	ed 1	L92	.168	3.7	.25	:502	293			-					
Pattern d	lata	has	s be	een	ver	rifi	ied.	, ar	nd								
Showing R	tx da	ata	cor	nter	nt v	vit	n tl	ne t	firs	st d	data	a o'	ffse	et a	at 0	9×00	0029BF4
Address	0	1	2	3	4	5	6	7	8	9	а	b	С	d	е	f	
00029BF0	FØ	F1	F2	F3	00	00	00	00	00	00	01	F4	<b>0</b> 8	09	ØA	ØB	
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	ЗA	3B	
00029C30	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	<b>4</b> A	<b>4</b> B	
00029C40	4C	4D	<b>4</b> E	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	<b>8</b> A	8B	
00029C80	8C	8D	8E	8F	90	91	92	93	94	95	96	97	98	99	9A	9B	
00029C90	9C	9D	9E	9F	AØ	A1	A2	Α3	Α4	A5	A6	A7	<b>A8</b>	A9	AA	AB	
00029CA0	AC	AD	AE	AF	BØ	B1	B2	<b>B</b> 3	<b>B4</b>	B5	<b>B6</b>	Β7	<b>B8</b>	B9	ΒA	BB	
00029CB0	BC	BD	BE	BF	C0	C1	C2	<b>C</b> 3	C4	C5	<b>C</b> 6	<b>C7</b>	<b>C8</b>	<b>C</b> 9	CA	CB	
00029CC0	CC	CD	CE	CF	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	
00029CD0	DC	DD	DE	DF	EØ	E1	E2	E3	<b>E4</b>	E5	E6	E7	<b>E8</b>	E9	EA	EB	
00029CE0	EC	ED	EE	EF	FØ	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	ØA	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	ЗA	3B	
00029D30	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	<b>4</b> B	
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	<b>8</b> A	8B	
00029D80	8C	8D	<b>8</b> E	8F	90	91	92	93	94	95	96	97	98	99	9A	9B	
00029D90	9C	9D	9E	9F	AØ	A1	A2	<b>A</b> 3	A4	A5	<b>A6</b>	A7	<b>A8</b>	A9	AA	AB	
00029DA0	AC	AD	AE	AF	BØ	B1	B2	<b>B</b> 3	B4	B5	<b>B6</b>	Β7	<b>B8</b>	B9	ΒA	BB	
00029DB0	BC	BD	BE	BF	C0	C1	C2	<b>C</b> 3	C4	C5	<b>C6</b>	<b>C</b> 7	<b>C8</b>	<b>C</b> 9	CA	CB	
00029DC0	CC	CD	CE	CF	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	
00029DD0	DC	DD	DE	DF	EØ	E1	E2	E3	E4	E5	E6	E7	<b>E8</b>	E9	EA	EB	
00029DE0	EC	ED	EE	EF	FØ	F1	F2	F3	E8	E9	EA	EB	EC	ED	EE	EF	
There with the constant of the																	
Transmitting Speed 1.230 Mops																	
lotal tra	inste	er s	51Z(	3 =	500	a Bì	/τe	(s)									
Receiving	; spe	eed	12		12	nop	5										
				111													

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
       0123456789abcdef
Address
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.
- Batch file named "QUIC10GSIPTest.bit" and "QUIC10GCIPTest.bat" (To download these files, please visit our website at <u>www.design-gateway.com</u>)



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.





### 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.







### 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.

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	-

#### Table 1 QUIC10GS-IP Performance test result



## 9 Revision History

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