

# **TLS10GC-IP Demo Instruction**

1	Environment Setup								
2	PC Setup	4							
	2.1 IP setting	4							
	2.2 Speed and duplex setting	5							
	2.3 Network properties setting	6							
3	Node.js server	9							
4	Test software on PC	13							
5	Client web browser	14							
6	Board Setup	17							
7	Serial Console	18							
8	Command Details	19							
	8.1 Set FPGA's IP Address	19							
	8.2 Set FPGA's Port Number	19							
	8.3 Set FPGA's MAC address	19							
	8.4 Set Gateway's IP Address	19							
	8.5 Enable showkey mode	19							
	8.6 Enable showcert mode	20							
	8.7 Download data	22							
	8.8 Upload data	23							
	8.9 Full duplex test	24							
9	Test setup when using 2 FPGA boards	25							
	9.1 Environment setup when using 2 FPGA boards	25							
	9.2 Test sequence	26							
	9.2.1 Set parameters and start a server	26							
	9.2.2 Transmit data test (Server to client)	26							
	9.2.3 Receive data test (Client to server)	27							
	9.2.4 Full duplex test	27							
10	Test results	28							
	10.1 Functionality testing	28							
	10.2 Performance testing	30							
11	Revision History	32							



# **TLS10GC-IP Demo Instruction**

#### Rev1.03 2-Apr-2025

This document describes the instruction to demonstrate the operation of TLS1.3 Client 10Gbps IP Core (TLS10GC-IP) on ZCU106 Evaluation Board. In this demonstration, TLS10GC-IP is used to establish a secure connection using the Transport Layer Security protocol version 1.3 over TCP. This involves handling the TLS1.3 handshake, encrypting and decrypting data transferred between the user and server. Additionally, HTTPS is selected as the application layer protocol to simplify the testing of data transfer between a standard server and the TLS10GCdemo.

This instruction explains the process for users to use TLS10GCdemo as a client for uploading or downloading data patterns from the provided example node.js server, obtaining results similar to use a web browser. This instruction also covers the use of the "server" application to test transfer speed between a PC and TLS10GCdemo, as well as the comparison of test results between two FPGA boards.

#### 1 Environment Setup

To operate TLS10GC-IP demo, please prepare following test environment.

- 1) FPGA development board: ZCU106 or KCU116 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 ZCU106 board and Test PC.
- 5) Micro USB cable for UART connection connecting between ZCU106 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 these files, please visit our web site at <u>www.design-gateway.com</u>)





Figure 1 TLS10GCIP demo environment on ZCU106 board



Figure 2 TLS10GCIP 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	E SFP+	You can get IP settings assigned automatically if you this capability. Otherwise, you need to ask your net for the appropriate IP settings.	ır network supports work administrator
	Configure	Obtain an IP address automatically	
his connection uses the following items:		Use the following IP address:	
Client for Microsoft Networks	^	IP address: 192 . 168	. 11 . 25
<ul> <li>The and Printer Shaning for Microsoft Ne</li> <li>Pipeap Packet Driver (NPCAP)</li> </ul>	tworks	Subnet mask: 255.255	. 255 . 0
QoS Packet Scheduler     Internet Protocol Version 4 (TCP/IPv4)	2	Default gateway:	
Microsoft Network Adapter Multiplexor F     Microsoft LLDP Protocol Driver	Protocol	Obtain DNS server address automatically	192 . 168 . 11 . 25
<	>	• Use the following DNS server addresses:	
Install	Properties	Preferred DNS server:	
Description		Alternate DNS server: .	
Transmission Control Protocol/Internet Protoco wide area network protocol that provides com across diverse interconnected networks.	ol. The default munication	Validate settings upon exit	Advanced
OK	Cancel		Cance

Figure 3 Setting IP address for PC

- 1) Open Local Area Connection Properties of 10 Gb connection, as shown in the left window of Figure 3.
- 2) Select "TCP/IPv4" and then click Properties.
- 3) Set IP address = 192.168.11.26 and Subnet mask = 255.255.255.0, as shown in the right window of Figure 3.



## 2.2 Speed and duplex setting



#### Figure 4 Set Link Speed = 10 Gbps

- 1) On Local Area Connection Properties window, click "Configure", as shown in Figure 4.
- 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 4.



## 2.3 Network properties setting

Some of network parameter setting may affect to network performance. The example of network properties setting 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 5.

ntel(R) E	thernet Con	troller X7	10 for 1	OGbE SF	P+ Propertie	es >
General	Advanced	Driver	Details	Events	Power Mana	agement
The foll the prop on the r Property	owing propert berty you wan ight. /:	ies are ava t to chang	ailable fo le on the	orthisne eleft, and Va	twork adapter. I then select it alue:	. Click s value
Enable Energy Row C Interrug IPv4 C Jumbo Large : Large : Large : Locally Log Lir Maximu	PME Efficient Ethion ontrol of Moderation hecksum OffI Packet Send Offload Send Offload Send Offload ate on Interfa Administered nk State Ever um Number of um Number of	emet Rate oad V2 (IPv4) V2 (IPv6) V2 (IPv6) I Address it f RSS Prod f RSS Que			Disabled Disabled Enabled	~
					ОК	Cancel

Figure 5 Interrupt Moderation



2) On "Interrupt Moderation Rate" window, set value to "OFF", as shown in Figure 6.



#### Figure 6 Interrupt Moderation Rate

3) On "Jumbo packet" window, set value to "9014 Bytes", as shown in Figure 7.

Intel(R) Ethernet Controller X710 for 10GbE SFP+ Properties							
General	Advanced	Driver	Details	Event	s Power Mar	nagement	
The foll the proj on the i Property Enable Energy Flow C Interru Interru IPv4 C Jumbo Large Large Large Large Locally Locally Locally Maxim	owing propert perty you wan ight. y: PPME / Efficient Eth- control pt Moderation pt Moderation pt Moderation pt Moderation Packet Send Offload Send Offload Send Offload send Offload tate on Interfa / Administered um Number of um Number of	ies are a t to char emet Rate oad V2 (IPv4 V2 (IPv4) V2 (IP	vailable f ige on the i) i) i) ocessi jeues V	or this n e left, ar	etwork adapte nd then select Value: 9014 Bytes 9014 Bytes 9014 Bytes Disabled	er. Click its value	~
					ОК	Can	cel





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

Intel(R) E	thernet Con	troller X	710 for 1	OGbE SFI	P+ Propertie	s	×
General	Advanced	Driver	Details	Events	Power Mana	gement	
The foll the prop on the r	Click value						
Property	<i>r</i> :			Va	lue:		
Link St Locally Log Lir Maximu Maximu Packet Preferm	ate on Interfa Administered Na State Ever Um Number of Um Number of Thiority & VL ed NUMA no	ace Down IAddress nt FRSS Pro FRSS Qu AN de			096		•
Receiv Receiv RSS B RSS lo Speed	Preferred NUMA node Receive Buffers Receive Side Scaling RSS Base Processor Number RSS load balancing profile Speed & Durplay						
TCP C TCP C	hecksum Offl hecksum Offl	oad (IPv4 oad (IPv6	4) 5) ~				
				_			
					ОК	Can	icel

#### **Figure 8 Receive Buffers**

5) On "Transmit Buffers" window, set value to the maximum value, as shown in Figure 9.

Intel(R) Ethernet Controller X710 for 10GbE SFP+ Properties									
General	Advanced	Driver	Details	Events	Power Mana	gement			
The foll the prop on the r	The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.								
Property	y:			Va	alue:				
Maximi Packe Preferr Receiv RSS B RSS Io Speed TCP C TCP C TCP C UDP 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 hecksum Offi hecksum Offi ID	FRSS Qu AN de g r Numbe profile oad (IPv oad (IPv load (IPv	r 4) 5) 4)		1096				
				E	ОК	Canc	el		

Figure 9 Transmit Buffers



### 3 Node.js server

In this demonstration, a sample server is created using Node.js. The server opens port 60001 for HTTPS connection. The required files for running the server are provided in server folder which contains the file as follow,

- 1) serverDemo.js for running server.
- 2) key.pem and cert.pem as a sample RSA key information and server's certificate.
- 3) uploadMenu.html for making web browser can upload data to server via POST method.
- 4) server/log folder for containing files, DG.html, bike.html, pinkpanther.html and rex.html. Users can add files to server/log folder to be the resource for downloading.

When serverDemo.js is executed\*, IP address and port number of server are displayed on console, as shown in Figure 10.



#### Figure 10 Server console when serverDemo.js is executed

#### Caution

When testing serverDemo.js with TLS10GCdemo, the FPGA board must be programmed before executing serverDemo.js to ensure that the server can detect the Ethernet interface between the FPGA board and the PC and can communicate properly.



By default, serverDemo.js does not verify data to optimize transfer speed. However, users can enable the data verification feature by including the "-v" parameter when executing serverDemo.js, as shown in Figure 11.



#### Figure 11 Server console when enabling verifying data

In case of client cannot access node.js server, please check firewall setting as below,

- 1) Go to Windows Defender Firewall with Advanced Security
- 2) Click on "Inbound Rules"
- 3) Search for "Node.js JavaScript Runtime" and open its properties
- 4) Go to "Protocols and Ports" tab and set Protocol type = TCP, Local port = Specific Ports that server on PC open. By default, the sample server opens port 60001. Local port number is set to 60001, as shown in Figure 12.
- 5) Go to "Advanced" tab and mark the profile boxes that match the network profile of ethernet card, as shown in Figure 13.



Genera	al	Programs a	and Services		Remot	e Computers
Protocols and Ports Scope			Advanced	Local F	Principals	Remote User
Protocol	s and ports					
and the	Protocol t	ype:	TCP			~
	Protocol	number:		6 🔹		
Local port:		t:	Specific P	orts		~
		60001				
			Example:	80, 443,	5000-5010	)
	Remote p	oort:	All Ports			~
			Example:	80. <mark>44</mark> 3.	5000-5010	)
	Internet C (ICMP) se	Control Messag ttings:	ge Protocol		Customia	ze

Figure 12 Protocols and Ports setting

Node.js JavaScript Runtime Properties							$\times$	
General Programs and Services Remote Computer								
Protocols an	d Ports	Scope	Advanced	Loca	l Principals	Remote Users		
Profiles	Specify pr ☐ Doma ☑ Private ☑ Public	ofiles to wh in e	nich this rule app	olies.				
	types Specify th rule applie	e interface s.	types to which	this	Customiz	e		
Edge trav	ersal							
	Edge trave inbound p such as a firewall.	ersal allows ackets tha Network A	the computer t t have passed t ddress Translat	o acce hrough ion (N	ept unsolicited an edge dev AT) router or	ł rice		
	Block edg	ge traversa			~			
Prevent applications from receiving unsolicited traffic from the Internet through a NAT edge device.								
			OK		Cancel	Apply		

Figure 13 Advanced setting



Clients can download data patterns or existing files in the server/log folder by sending a GET command with URL.

For downloading data pattern, there are 4 data patterns which are increasing binary, decreasing binary, increasing text and decreasing text pattern. When a server receives a GET request, data pattern and length of requested data are displayed on the server console, as shown in Figure 14.



Figure 14 Server console when client download data pattern

For downloading html file in server/log folder, when a server receives a GET request, file path of requested data is displayed on the server console, as shown in Figure 15.



Figure 15 Server console when client download ./log/DG.html

Clients can upload data to the server by sending a POST command followed by uploaded data. After completely transferring, received data, length of data and transfer speed are displayed on the server console, as shown in Figure 16. If data length is more than 16 kB, the server console shows only data length and transfer speed.



Figure 16 Server console when client upload data



## 4 Test software on PC

Due to the encrypting/decrypting process in the TLS protocol, Node.js server on the PC cannot achieve full-speed data transfer between PC and TLS10GC-IP. The "server" application is designed to run on the PC similar to the Node.js server for testing the performance of TLS10GC-IP via ethernet. The server opens port 60001 for HTTPS connection. Users can select the ethernet IP address for testing corresponding to the IP address of the 10 Gb Ethernet card, as shown in Figure 17.



Figure 17 Server application console

For upload speed testing, after the handshake process is completed, "server" application will receive TxData from the client and count the number of received data to validate whether it matches the value form the URL. To achieve optimal data transfer speed, the received data will remain undecrypted and unverified. Then the transfer speed is displayed on the server console, as shown in Figure 18.

For download speed testing, after the handshake process is completed, "server" application will prepare the encrypted data pattern corresponding to the data pattern from the URL and continuously send it to the client. The download speed will be displayed on the server application console, as shown in Figure 19.

```
Client upload data length : 2147483647 Byte
Received data: 2147483647 Byte success.
Thoughtput 9179.92 Mbps
```

Figure 18 Server application console when testing upload speed

Client download length : 2147483647 Byte Generate Data: 2147483647 Byte Success! Transmitted data: 2147483647 Byte Success! Thoughtput 9130.08 Mbps

Figure 19 Server application console when testing download speed

#### 5 Client web browser

Users can use a web browser for downloading data from server by GET method and uploading data to the server via POST method.

For downloading data pattern, user can input URL in the following format,

https://ip:port/direction/pattern/length

Where	ip	represent server's IP address in do	-decimal notation					
	port	represent server's port number						
	direction represe	ent download or upload						
	pattern	represent data pattern						
		b1: increasing binary pattern,	t1: increasing text pattern,					
		b0: decreasing binary pattern,	t0: decreasing text pattern					
	length	represent data length in byte						

As shown in Figure 20, server's IP address is 192.168.7.26, port number is 60001 and the user's URL is https://192.168.7.26:60001/download/t1/123. Secure connection is established, the 123-byte increasing text pattern is displayed in the web browser.

•	<b>③</b> 1	92.168.7	7.26:60001/downlo	ad/t ×	+									_		×
÷	$\rightarrow$	G	Not secure	https://	192.168	8.7.26:60	0001/do	ownloa	ad/t1/	123	☆		Ĵ			:
01234 @ABCI	456789 DEFGHI	):;<=>? []KLMNC	@ABCDEFGHIJKLI PQRSTUVWXYZ[\]	MNOPQRST ]^_`abcd	UVWXYZ[ efghij	`\]^_`a	abcdefg	hijkl	mn001	2345678	39:;<=	>?				

#### Figure 20 Increasing text pattern shown in web browser

#### <u>Remark</u>

- Our tested web browser is Google Chrome version 116.0.5845.141.
- The RSA certificate used in this demonstration is self-signed, meaning it was not issued by a certification authority (CA). When attempting to access the server with a self-signed certificate, the web browser may display a "Not Secure" alert.
- In case of downloading a binary pattern, a "Save as" dialog window appears. Users can save the file and view the binary data after the download process is complete.



For downloading existing files in server/log folder, users can input URL in the following format,

https://ip:port/download/log/filename

When user inputs https://192.168.7.26:60001/download/log/DG.html and DG.html exists in log folder. The secure connection is established, the html page is downloaded and displayed on the web browser, as shown in Figure 21.



Figure 21 DG.html shown in web browser

Users can securely upload data through web browser by requesting uploadMenu.html from https://192.168.7.26:60001/upload/menu. Upload menu is displayed in the web browser, as shown in Figure 22. Users can select the data pattern and data length. The HTML page will prepare the data and send a POST command along with the data pattern to the server when the "POST" button is pressed. Because the length of the data is greater than or equal to 16,000 bytes, only the data length and transfer speed are displayed on server console when the upload is completed, as shown in Figure 23.

TLS10GC IP Core	
<ul> <li>✓ S 192.168.7.26:60001/upload/mer</li> <li>× +</li> </ul>	– 🗆 ×
← → C ⊗ Not secure https://192.168.7.26:60001/upload/m	nenu 🖈 🖸 🗖 😩 :
Upload menu choose your data pattern. DataPattern : Increasing v binary v DataLength : 5 byte(s) POST	
Figure 22 Secured upload	page



Figure 23 Server's console when client upload large data

#### 6 Board Setup

Follow these steps to set up the ZCU106 FPGA development board:

- 1) Make sure power switch is off and connect power supply to FPGA development board.
- 2) Connect two USB cables between FPGA board and PC via micro-USB ports.
- 3) Power on system.
- 4) Download configuration file and firmware to FPGA board by following step,
  - a) open Vivado TCL shell.
  - b) change current directory to download folder which includes demo configuration file.
  - c) Type "TLS10GCTest.bat", as shown in Figure 24.



#### Figure 24 Example command script for download configuration file

Follow these steps to set up the KCU116 FPGA development board:

- 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	HARDWARE MANAGER
File Flow Iools Window Help Q-Quick Access	ii) Open target -> Auto Connect
	Hardware     Ø     Auto Connect       Q     素     ♦     Ø       Auto Connect     Recent Targets     ♦       Auto Connect     Available Targets on Server     ♦       Open New Target     Open New Target     ●
Quick Start	
Quick Stall	HARDWARE MANAGER - localhost/xilinx_tcf/Digilent/210308AB9D59
Create Project >	Hardware ? _ 🗆 🖾 🗙 MIG - MIG_1
Open Project >	
Open Example Project >	Name Status V II localhost (1) iii) Select FPGA device to program bit file
Tasks	Verify Device     Verify Device.     Verify
Open Hardware Manager > Vivado Store >	Select a bitstream programming file and download it to your
Learning Center Documentation and Tutorials > Quick Take Videos > What's New in 2021.1 >	file that corresponds to the debug cores contained in the bitstream programming file. Bitstream file: Debug probes file: vi) Click Program button to start FPGA Programming v) Brogram Cance

#### Figure 25 Program Device



#### 7 Serial Console

Users can set the parameters, download and upload data by using the following command. The TLS10GCdemo commands and their usage will be displayed, as shown in Figure 26. Detailed information about each command is described in Topic 8 Command Details.

```
TLS10GC version 0x80011843

wait_ethlink

Usage:

[1] setip ddd.ddd.ddd.ddd

Set FPGA's IP address in dotted-decimal format.

[2] setport ddddd

Set FPGA's port number in decimal format or type dynamic/d/-d to set dynamic port number.

[3] setmac hh-hh-hh-hh-hh

Set FPGA's MAC address in hexadecimal format.

[4] setgateway's IP address in hexadecimal format.

[5] showkey (1: enable, 0: disable>

Enable showkey mode for show TLS traffic ticket, session key and iv for encryption/decryption.

[6] showcert (1: enable, 0: disable>

Enable showcert mode for show certificate infomation.

[7] myGET https://ip:port/download/pattern/length

Send GET command for downloading pattern data from server.

[8] myPOST https://ip:port/fullduplex/pattern/length

Test fullduplex with test software.

>>
```

Figure 26 Serial console



## 8 Command Details

## 8.1 Set FPGA's IP Address

command> setip ddd.ddd.ddd.ddd

This command is used to set FPGA's IP address in dotted-decimal format. The default FPGA's IP address is 192.168.11.42. Users can input setip command followed by a valid IP address.

## 8.2 Set FPGA's Port Number

command> setport ddddd

This command is used to set the static port number of FPGA in decimal format. By default, the FPGA's port number is set to be dynamic. Dynamic ports range from 49152 to 65535. Users can enable dynamic port again after specifying a port number by using "setport dynamic" command.

#### 8.3 Set FPGA's MAC address

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

```
This command is used to set FPGA's MAC address in hexadecimal format. The default FPGA's MAC address is 00-01-02-03-04-05.
```

#### 8.4 Set Gateway's IP Address

command> setgatewayip ddd.ddd.ddd.ddd

This command is used to set gateway's IP address in dotted-decimal format. The default gateway's IP address is 192.168.11.2. Users can input setgatewayip command followed by a valid IP address.

#### 8.5 Enable showkey mode

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

This command is used to enable showkey mode. When showkey mode is enabled, the TLS traffic ticket for encryption/decryption is displayed on the serial console, as shown in Figure 27. Users can use the TLS traffic ticket as (Pre)-Master-Secret log file for Wireshark\* to decrypt transferred data between the client and server.

#### Figure 27 Serial console when showkey mode is enabled

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



#### 8.6 Enable showcert mode

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

This command is used to enable showcert mode. When showcert mode is enabled, the server's certificate stored in CertRam is displayed on the serial console, as shown in Figure 28. The certificate information is displayed in hexadecimal format, which corresponds to the result obtained by using openssl command: openssl x509 -in cert.pem -outform der | hexdump -C, as shown in Figure 29.

3 $3$ $6$ $0$ $0$ $3$ $5$ $3$ $0$ $3$ $5$ $3$ $0$ $3$ $3$ $0$ $0$ $0$ $0$ $3$ $5$ $3$ $0$ $0$ $0$ $1$ $0$ $0$ $1$ $0$ $0$ $0$ $1$ $0$ <th colspan="10"> Certificate infomation</th>	 Certificate infomation																
82       02       3B       A0       03       02       01       02       14       50       10       DD       BC       F4       A8         3C       39       69       76       11       E8       B2       A0       CA       2B       C5       67       89       A3       00       B0       30       38       31         08       30       09       06       03       55       04       06       13       02       54       48       31       10       30       08       31       30       32       33       30       32       33       30       32       33       30       32       33       30       32       32       33       30       32       32       33       30       32       33       30       32       33       30       32       33       30       32       33       30       32       32       33       30       32       32       33       30       32       33       30       32       32       33       30       32       32       33       30       32       32       33       30       32       32       32		ØB	00	03	60	00	00	03	5C	00	03	57	30	82	03	53	30
3C 37 69 76 11 E8 B2 H0 CH 28 C5 67 87 8H 30 01 0B 30 09 06 03 55 04 06 13 02 54 48 31 10 30 0E 06 03 55 04 08 0C 07 42 61 6E 67 6B 6F 6B 31 17 30 15 06 03 55 04 04 00 C0 24 46 55 73 69 67 62 20 47 61 74 65 77 61 79 30 20 17 0D 32 33 30 32 32 34 30 39 32 38 31 30 5A 18 0F 32 31 32 33 30 32 33 31 30 39 32 38 31 30 5A 18 0F 32 31 32 33 30 32 35 04 0A 0C 0E 44 65 73 69 67 6E 20 47 61 74 65 77 61 79 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 00 C0 36 8C 0A DC 4F BF 0B 1C 40 3C 77 17 FF B8 11 F3 C5 02 20 D2 F7 C0 AC A 96 CA D0 CD 3F 88 48 C1 87 FC F3 B7 13 5E 29 B6 C9 96 19 F4 ED BC C2 8D EB AF F6 92 0A A2 B9 93 5C CF 34 BD 1B 8C D1 24 54 7F 59 6B 01 5A 22 40 94 63 8F 2B 24 4F 07 64 36 D7 75 75 67 77 22 61 68 67 55 77 64 0A 0C D2 3F 88 48 C1 87 FC F3 B7 13 5E 29 B6 C9 96 19 F4 ED BC C2 8D EB AF F6 92 0A A2 B9 93 5C CF 34 BD 1B 8C D2 39 72 11 6B 01 5A 22 40 94 63 8F CB 34 13 60 72 96 23 97 21 6B 01 5A 22 40 94 63 8F CB 41 36 67 29 66 39 51 D6 24 53 7C 81 67 FD BF 70 F 8F 03 07 2E 89 75 76 10 97 2A FB 55 14 B8 98 EB F7 DF 8F 03 07 2E 80 C4 36 D7 AF 55 14 B8 98 EB F7 DF 8F 03 07 2E 80 C4 39 6D 74 26 55 12 CF 75 F7 97 2A FB 5E 4D 75 80 64 43 6D 75 FF 69 20 93 11 D0 90 73 44 6C 53 C0 BD A2 89 1E 4E 59 75 9F 17 D 86 8A A55 358 11 E 63 C0 BD A2 89 1E 4E 59 75 9F 10 B 19 A9 A8 95 34 00 7E 83 F1 68 6C 59 CA 49 1D 99 D7 34 4C 53 C0 BD A2 89 1E 4E 59 75 9F 15 A 78 9D 85 3C FB C8 72 69 1F D1 97 E1 97 E1 75 54 78 9D 85 3C FB C8 72 69 1F D1 97 E1 97 E1 76 62 F5 DF AE 30 1F 06 63 55 1D 02 04 16 04 14 DA 27 4C 41 24 45 7B 02 D8 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 1F 76 06 30 55 1D 02 04 16 04 14 DA 27 4C 41 24 45 7B 02 D8 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 1F 06 03 55 1D 02 04 16 04 16 04 14 DA 27 4C 41 24 45 7B 02 D8 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 1F 06 03 55 1D 02 04 16 04 16 80 14 DA 27 4C 41 24 45 7B 02 D8 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 1F 06 03 55 1D 23 04 16 01 0F 70 0B 24 29 7C 24 24 45 79 22 40 4D 54 28 86 F7 0D 0B 14 00 85 00 33 01 01 FF 30 0F 06 09 24 74 74 15 50 7A 70 B D4 30 EB 2A 29 79 CE D1 73 78 2		82	02	3B	AØ	03	02	01	02	02	14	50	10	DD	BC	F4	A8
30 $30$ $00$ $03$ $55$ $04$ $00$ $13$ $02$ $54$ $48$ $31$ $10$ $30$ $10$ $06$ $03$ $55$ $04$ $08$ $0C$ $07$ $42$ $61$ $6E$ $73$ $69$ $66$ $83$ $17$ $00$ $32$ $33$ $30$ $32$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $33$ $30$ $32$ $33$ $30$ $33$ $30$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $33$ $30$ $32$ $32$ $32$ $32$ $32$ $32$ $32$ $32$ $32$ $32$ $32$		30	37	20	26	11 48	E8 86	B2 F7	нø Øn	CH Ø1	2B Ø1	GS ØR	67	87 00	8H 30	30	ОD 31
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		ЙB	зó	<b>Ø</b> 9	<b>0</b> 6	03	55	04	06	13	02	54	48	31	10	30	ØĒ
30 15 06 03 55 04 0A 0C $0E$ 44 65 73 69 67 6E 20 47 61 74 65 77 61 79 30 20 17 0D 32 33 30 32 32 33 31 30 39 32 38 31 30 5A 18 0F 32 31 32 33 30 32 32 33 55 04 06 13 02 54 48 31 10 30 0E 06 03 55 04 08 0C 07 42 61 6E 67 6B 6F 6B 31 17 30 15 06 03 55 04 06 10 0E 44 65 73 69 67 6E 20 47 61 74 65 77 61 79 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 C0 36 8C 0A DC 4F BF 0B 1C 40 3C 77 17 EF BB 81 F3 C5 02 D2 F7 CA CA 96 CA D0 CD 3F 0B 48 C1 87 FC F3 B7 13 5E 29 B6 C9 96 19 F4 ED BC C2 8D EB AF F6 92 0A A2 B9 93 5C CF 34 BD 1B 3C D1 24 54 75 59 6B 75 9F F7 00 EE 38 4A 13 60 72 96 23 97 21 6B 01 5A 22 40 94 63 8F 2B 24 4F 07 64 36 07 AF 55 14 B8 98 EF7 DF 8F 03 07 2E B8 64 78 73 17 18 A4 7B 79 2A FB 5E 4D 75 06 C4 43 62 BA C7 5F A9 72 E5 8E 74 C5 AE B5 FE 98 65 49 D3 7F C0 DE 39 31 9D 06 38 AC FA AD 68 44 00 3A B9 51 D6 24 53 7C 81 67 FD DB 19 A9 A8 53 34 00 7E 83 F1 68 6C 59 CA 49 1D 99 D7 34 4C 56 01 2A 38 7F C0 Z2 CB C8 83 4B AA 53 30 51 30 1D 06 63 55 1D 0E 04 16 04 14 DA 27 4C 41 24 45 7B 07 64 36 07 2F 83 F1 68 6C 59 CA 49 1D 99 D7 34 4C 56 01 2A 38 7F 12 S AA 25 D2 CB EF PD AE 30 A15 40 53 55 1D 0E 04 16 04 14 DA 27 4C 41 24 45 7B 08 55 34 00 7E 83 F1 68 6C 79 FA 1D 87 A3 30 51 30 1D 06 3 55 1D 02 04 18 30 16 80 14 A3 53 30 51 30 1D 06 3 55 1D 02 04 18 30 16 80 14 A0 27 4C 41 24 45 7B 09 20 35 1D 13 01 10 FF 49 00 30 C9 31 35 35 85 B8 84 0D 61 A0 25 C0 47 7B 75 8F 9F 02 03 01 00 01 A3 53 30 51 30 1D 06 79 34 29 7D B8 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 0F 18 02 09 A9 58 0B 6C 13 EC 74 F9 6E FF DF AE 30 0F 06 03 55 1D 02 04 18 30 16 80 14 DA 27 4C 41 24 45 7B 09 20 85 80 0B 6C 13 EC 74 F9 6E EF DF AE 30 0F 04 09 30 C9 31 35 35 85 B8 84 0D 61 A0 25 C0 77 7B 75 8F 9F 02 03 01 01 FF 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 86 05 00 63 82 01 01 00 3D C9 31 35 55 B8 84 0D 61 A0 25 CC 47 7B 75 8F 9F 02 25 3C F2 1F BD AA 32 02 2F EB 21 CB 79 A0 45 DA 58 15 ED 35 A2 6F 60 0F 47 B9 B8 A8 79 DC 40 7F 15 8D 57 A7 76 BB 49 30 FB 82 79 92 6E 67 67 20 6F 33 C2 93 A0 45 D		06	03	55	04	08	ØČ	07	42	61	6Ē	67	6B	6F	6B	31	17
47 $61$ $74$ $65$ $77$ $61$ $77$ $30$ $22$ $81$ $17$ $90$ $32$ $33$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $31$ $30$ $30$ $32$ $33$ $30$ $31$ $30$ $30$ $32$ $31$ $32$ $33$ $30$ $31$ $30$ $31$ $30$ $32$ $31$ $32$ $31$ $32$ $31$ $30$ $30$ $32$ $31$ $30$ $31$ $30$ $30$ $32$		30	15	<u>Ø6</u>	03	55	04	ØA	ØC	ØE	44	65	73	69	67	6E	20
33       31       30       32       38       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       36       31       30       35       30       35       31       30       35       31       30       35       31       30       32       30       32       31       30       35       31       30       35       30       35       31       30       35       30       35       31       30       35       36       31       30       35       36       31       30       35       36 <t< td=""><th></th><td>47</td><td>51 30</td><td>29</td><td>55</td><td>38</td><td>61 31</td><td>30</td><td>30 50</td><td>20</td><td>17 ØF</td><td>32</td><td>32</td><td>33</td><td>30</td><td>32</td><td>32</td></t<>		47	51 30	29	55	38	61 31	30	30 50	20	17 ØF	32	32	33	30	32	32
93       55       04       06       13       02       54       48       31       10       30       0E       06       03       55       04         08       0C       07       42       61       6E       67       68       31       17       30       15       06       03         57       61       79       30       82       01       22       30       0D       06       09       2A       86       48       86       F7         0D       01       01       00       03       82       01       0F       00       30       82       01       00       20       86       48       86       F7         01       01       00       03       82       01       0F       00       30       82       01       00       20       20       10       10       00       00       30       82       01       00       30       82       01       00       30       77       61       74       65       01       03       82       04       01       00       00       00       00       00       00       00       01		33	31	зó	39	32	38	31	30	<b>5</b> Å	30	38	31	ЙВ	30	<b>0</b> 9	ØĠ
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		03	55	04	06	13	02	54	48	31	10	30	ØE	06	03	55	04
35       64       66       64       86       67       67       66       20       47       61       74       65         97       61       91       06       06       23       82       01       06       09       20       86       48       86       67         90       01       01       00       00       38       201       00       60       30       82       01       00       20       23       82       01       00       00       30       82       01       00       00       30       82       01       00       00       20       27       76       00       01       01       00       00       00       20       27       76       00       00       00       00       00       01       01       01       01       01       01       01       00       00       00       20       01       01       01       01       01       01       00       02       01       01       01       01       01       01       01       01       01       01       01       01       01       01       01       01       01		<u>Ю8</u>	ЮC	Ø7	42	61	6E	62	6B	6F	éB	31	17	30	15	<b>96</b>	03
10010101010201010382010101020101028201010000368C0ADC4FBF0B1C403C7717EFBB81F3C502D2P7CACA96CAD0D124547F5796879797F166C996C7961382019724547F59687597F700EE384A1360729623972168015A224094638522244F076436D7AF5514B89888BF7DDF8F030722EB97E86478731718A47B792AFB5E4D7506C44362BAC75FA9722E58E74CAAAA759685319D0638ACFAAD6864AB53585110686C59CA4910977344C56012A8371686C59 <t< td=""><th></th><td>55 77</td><td>61</td><td><u>өн</u> 79</td><td>30</td><td>82</td><td><u>яч</u> Й1</td><td>22</td><td>30</td><td>ЙĎ</td><td>ЙŔ</td><td><u>й9</u></td><td>20</td><td>86</td><td>48</td><td>86</td><td>63 F7</td></t<>		55 77	61	<u>өн</u> 79	30	82	<u>яч</u> Й1	22	30	ЙĎ	ЙŔ	<u>й9</u>	20	86	48	86	63 F7
82010100C0368C0ADC4FBF0B1C403C7717EFBB81F3CS02D2F7CACA96CAD0D3F70B48C187FCF3B7135E29B6C99619F4ED8CC28DEBAFF6920AA2B9935CCF34BD1B3CD124547F596B759FF700EE388F2B244F076436077AF5514898EBF7DF8F93072EEB97E86478731718A47B792AFB5E4D7506C44362BAC75FA972E58E74C5AEB5E4D75986549D37FC0DE39319D90638ACFAAD6864D03AB951D624537C8167FDDB19A9A89534007E8371686659CA491D90727		ØĎ	Øī	01	õĭ	05	ŏô	03	82	01	ØF	ŏÓ	30	82	Õĭ	ØĂ	02
1717181173125102171611741750B48C187FCF3B7135E29B6C99619F4ED3CD124547F596B759FF700EE384A136072962397216B015A224094638F2B244F876436D7AF5514B898EBF7DF8F03072E866478731718A47B792AFB5E4D7596644362BAC75FA972E58E74C5AEB5FE986549D37FCODE39319D9638ACFAAD88641007E83F1686C59CA49D19D9D7344C56612A83D15C12CBC8834BAA535811E633C0BDA2891E4E59759154789D853CFBC872691D97F195 <t< td=""><th></th><td>82</td><td>01</td><td>01</td><td>00</td><td>CØ</td><td>36</td><td>80</td><td>ØA</td><td>DC</td><td>4F</td><td>BF</td><td>ØB</td><td>10</td><td>40</td><td>30</td><td>77</td></t<>		82	01	01	00	CØ	36	80	ØA	DC	4F	BF	ØB	10	40	30	77
BD       13       14       15       15       15       15       17       14       14       15         BC       12       45       17       15       15       15       15       14       15       17       14       15         BC       12       45       17       55       14       18       98       15       15       14       18       13       60         72       96       23       97       21       68       01       5A       22       40       94       63       8F       28       24       4F       97       26       15       14       18       98       18       77       DF       17       14       14       16       17       14       16       17       14       16       16       17       14       17       14       16       17       14       16       16       16       17       16       16       16       17       16       17       16       17       16       16       16       17       16       16       16       16       17       16       16       17       16       16       16       17	l	17 ØP	EF 40	BB	81	F3 FC	<b>C</b> 5	92	D2 1 2	F7	CA	GA	26	CA	DØ 19	GD	3F FD
3CD124547F596B759FF700EE384A136072962397216B015A224094638F2B244F076436D7AFF5514B898EBF7DF8F03072EEB97E86478731718A47B792AFB5E4D7596C44362BAC75FA9722E588E74C5AEB5FE986549D37FC0DE39319D90638AACFAAD6864D03AB951D624537C8167FDDB19A9A89534907E83F1686CA91DD9D7344C56012A83D15C12CBC8834BAA535811E633C0BDA2891E4E59759154789D853CFBC872691FD197E192PAAA25D2CBE8986213		BC	C2	8D	ĔŔ	AF	F6	92	ЙÅ	A2	<b>B9</b>	93	5C	ĊF	34	BD	1 B
729623972168015A224094638F2B244F $07$ 6436D7AF5514B898EBF7DF8F03072EEB97E86478731718A47B792AFB5E4D7596C44362BAC75FA972E58E74C5AEB5FE986549D37FC0DE39319D906638ACFAAD6864D03AB951D624537C8167FDDB19A9A89534907E83F1686CC59AP1D99D7344C56912A83D15C12CBC8834BAA53581E6633C0BDA2891E4E59759154789D853CFBC872691FD197E195AA22C2BE90A153343051301D0633551D866FB294A6533051		3Č	D1	24	54	7F	59	6B	75	9F	<b>F</b> 7	00	EE	38	46	13	60
b7 $b4$ $3b$ $D7$ $HF$ $5s$ $14$ $B8$ $98$ $EB$ $F7$ $DF$ $8F$ $b3$ $b7$ $22E$ $EB$ $97$ $E8$ $64$ $78$ $73$ $17$ $18$ $A4$ $7B$ $79$ $2A$ $FB$ $5E$ $4D$ $75$ $96$ $C4$ $43$ $62$ $BA$ $C7$ $5F$ $A9$ $72$ $E5$ $8E$ $74$ $C5$ $AE$ $B5$ $FF$ $98$ $65$ $49$ $D3$ $7F$ $C0$ $DE$ $39$ $31$ $9D$ $66$ $38$ $AC$ $FA$ $AD$ $68$ $64$ $D0$ $3A$ $B9$ $51$ $D6$ $24$ $53$ $7C$ $81$ $67$ $FD$ $DB$ $19$ $A9$ $A8$ $95$ $34$ $00$ $7E$ $83$ $F1$ $68$ $6C$ $75$ $75$ $91$ $54$ $78$ $9D$ $85$ $3C$ $FB$ $56$ $01$ $2A$ $83$ $p1$ $5C$ $12$ $CB$ $83$ $4B$ $AA$ $53$ $58$ $11$ $E6$ $72$ $E9$ $1F$ $p1$ $97$ $E1$ $95$ $AA$ $25$ $p2$ $CB$ $B8$ $90$ $A1$ $53$ $48$ $34$ $29$ $7D$ $B8$ $6F$ $B3$ $80$ $AA$ $CC$ $29$ $A8$ $57$ $B0$ $20$ $D8$ $58$ $D8$ $6C$ $13$ $EC$ $74$ $F9$ <		72	96	23	27	21	<u>6 B</u>	01	5A	22	40	24	63	8F	2B	24	4F
LD $77$ LB $67$ $71$ $16$ $77$ $12$ $57$ $27$ $C5$ $AE$ $B5$ $FE$ $98$ $65$ $49$ $D3$ $7F$ $C0$ $DE$ $39$ $31$ $9D$ $06$ $38$ $AC$ $FA$ $AD$ $68$ $64$ $D0$ $3A$ $B9$ $51$ $D6$ $24$ $53$ $7C$ $81$ $67$ $FD$ $DB$ $19$ $97$ $34$ $4C$ $56$ $01$ $2A$ $83$ $B1$ $5C$ $12$ $CB$ $C8$ $34$ $BA$ $53$ $58$ $11$ $E6$ $56$ $01$ $2A$ $83$ $D1$ $5C$ $12$ $CB$ $C8$ $34$ $BA$ $53$ $58$ $11$ $E6$ $56$ $01$ $2A$ $83$ $D1$ $5C$ $12$ $CB$ $C8$ $34$ $4B$ $AA$ $53$ $58$ $11$ $E6$ $72$ $C9$ $1F$ $D1$ $97$ $E1$ $95$ $AA$ $25$ $D2$ $CB$ $B8$ $90$ $A1$ $53$ $48$ $34$ $29$ $7D$ $B8$ $6F$ $B3$ $80$ $AA$ $CC$ $29$ $A8$ $D5$ $9C$ $82$ $47$ $B7$ $SF$ $PF$ $PF$ $AC$ $A1$ $24$ $45$ $7B$ $02$ $D8$ $58$ $B6$ $C1$ $12$ $P7$ $E6$ $FF$ $DF$ $AE$ $30$ $1F$ $06$ $35$ $1D$ $30$ </td <th></th> <td>EB</td> <td>64 97</td> <td>36 F8</td> <td>64</td> <td>HF 78</td> <td>55</td> <td>14</td> <td>18</td> <td>98</td> <td>ビビフロ</td> <td>F7 79</td> <td>DF 20</td> <td>8F FR</td> <td>03 5 F</td> <td>4D</td> <td>2E 75</td>		EB	64 97	36 F8	64	HF 78	55	14	18	98	ビビフロ	F7 79	DF 20	8F FR	03 5 F	4D	2E 75
98       65       49       D3       7F       CØ       DE       39       31       9D       06       38       AC       FA       AD       68         64       DØ       3A       B9       51       D6       24       53       7C       81       67       FD       DB       19       A9       A8         95       34       ØØ       7E       83       F1       68       6C       59       CA       49       1D       99       D7       34       4C         56       Ø1       2A       83       D1       5C       12       CB       C8       83       4B       AA       53       58       11       E6         33       CØ       BD       A2       89       1E       4E       59       75       91       54       78       9D       85       3C       FB         C8       34       29       7D       B8       6F       B3       80       AA       CC       29       A8       D5       9C       82       47         DB       75       91       54       78       9D       66       63       51       0D		06	ć4	43	62	BA	ćŽ	5ŕ	<b>Å</b> 9	72	É5	8É	<b>74</b>	C5	ĂĒ	<b>B</b> 5	FE
64       DØ       3A       B9       51       D6       24       53       7C       81       67       FD       DB       19       A9       A8         95       34       ØØ       7E       83       F1       68       6C       59       CA       49       1D       99       D7       34       4C         56       Ø1       2A       83       F1       68       6C       59       CA       49       1D       99       D7       34       4C         56       Ø1       2A       83       F1       68       6C       59       CA       49       1D       99       D7       34       4C         56       Ø1       A2       83       4B       AA       53       58       FD       D1       97       F1       97       AA       25       D2       CB       E8       90       A1       53         48       34       29       7D       B8       6F       B3       80       AA       CC       29       A8       D5       9C       82       47         DB       29       7D       B8       6F       B3       80		98	65	49	D3	7F	ĊØ	DE	39	31	9D	06	38	ĀČ	FA	ĀD	68
75 $34$ $00$ $7E$ $83$ $F1$ $68$ $6C$ $59$ $CH$ $49$ $1D$ $97$ $D7$ $34$ $4C$ $56$ $01$ $2A$ $83$ $D1$ $5C$ $12$ $CB$ $C8$ $83$ $4B$ $AA$ $53$ $58$ $11$ $E6$ $33$ $C0$ $BD$ $A2$ $89$ $1E$ $4E$ $59$ $75$ $91$ $54$ $78$ $9D$ $85$ $3C$ $FB$ $C8$ $72$ $69$ $1F$ $D1$ $97$ $E1$ $95$ $AA$ $25$ $D2$ $CB$ $E8$ $90$ $A1$ $53$ $48$ $34$ $29$ $7D$ $B8$ $6F$ $B3$ $80$ $AA$ $CC$ $29$ $A8$ $D5$ $9C$ $82$ $47$ $DB$ $75$ $8F$ $9F$ $02$ $03$ $01$ $00$ $01$ $A3$ $53$ $30$ $51$ $30$ $1D$ $06$ $03$ $55$ $1D$ $0E$ $04$ $16$ $04$ $14$ $DA$ $27$ $4C$ $41$ $24$ $45$ $7B$ $02$ $D8$ $6B$ $6C$ $13$ $EC$ $74$ $F9$ $6E$ $FF$ $DF$ $AE$ $30$ $0F$ $06$ $03$ $55$ $1D$ $13$ $01$ $01$ $FF$ $04$ $05$ $30$ $03$ $01$ $01$ $FF$ $30$ $0D$ $02$ $D8$ $86$ $48$ $86$ $F7$ $0D$ $01$ <t< td=""><th></th><td>64</td><td>DØ</td><td>3A</td><td><b>B9</b></td><td>51</td><td>D6</td><td>24</td><td>53</td><td><b>7</b>C</td><td>81</td><td>67</td><td>FD</td><td>DB</td><td>19</td><td>A9</td><td>A8</td></t<>		64	DØ	3A	<b>B9</b>	51	D6	24	53	<b>7</b> C	81	67	FD	DB	19	A9	A8
33 $C0$ BD $A2$ $87$ $16$ $12$ $59$ $75$ $91$ $478$ $9D$ $85$ $11$ $153$ $A8$ $34$ $29$ $7D$ $B8$ $6F$ $B3$ $80$ $AA$ $25$ $D2$ $CB$ $E8$ $90$ $A1$ $53$ $48$ $34$ $29$ $7D$ $B8$ $6F$ $B3$ $80$ $AA$ $CC$ $29$ $A8$ $D5$ $9C$ $82$ $47$ $DB$ $75$ $8F$ $9F$ $02$ $03$ $01$ $00$ $01$ $A3$ $53$ $30$ $51$ $30$ $1D$ $06$ $03$ $55$ $1D$ $0E$ $04$ $16$ $04$ $14$ $DA$ $27$ $4C$ $41$ $24$ $45$ $7B$ $02$ $D8$ $58$ $0B$ $6C$ $13$ $EC$ $74$ $F9$ $6E$ $FF$ $DF$ $AE$ $30$ $1D$ $06$ $03$ $22$ $D8$ $58$ $0B$ $6C$ $13$ $EC$ $74$ $F9$ $6E$ $FF$ $DF$ $AE$ $30$ $0F$ $06$ $03$ $55$ $1D$ $13$ $01$ $01$ $FF$ $04$ $05$ $30$ $03$ $01$ $01$ $FF$ $30$ $0D$ $02$ $D8$ $86$ $48$ $86$ $F7$ $0D$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$ $01$		95 56	34 01	20	2E 83	83 D1	F1 50	68 12	6C CR	57	6 8 3	49 4R	10	23	D7 58	34	4G F6
C8       72       69       1F       D1       97       E1       95       AA       25       D2       CB       E8       90       A1       53         48       34       29       7D       B8       6F       B3       80       AA       CC       29       A8       D5       9C       82       47         DB       75       8F       9F       02       03       01       00       01       A3       53       30       51       30       1D       06         03       55       1D       0E       04       16       04       14       DA       27       4C       41       24       45       7B       02         D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06       03       55       1D       13       01       01       FF       04       05       30       03       01       01       FF       30       0D       04       03       02       38       20       01       01       01       01       01       01       05       30		33	сø	BD	Å2	89	1Ĕ	4E	59	75	91	54	78	9D	85	3Ĉ	FB
48       34       29       7D       B8       6F       B3       80       AA       CC       29       A8       D5       9C       82       47         DB       75       8F       9F       02       03       01       00       01       A3       53       30       51       30       1D       06         03       55       1D       02       04       16       04       14       DA       27       4C       41       24       45       7B       02         D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06       03       55       1D       13       01       01       FF       04       05       30       03       01       01       FF       30       0D         04       10       01       03       03		<b>C8</b>	72	69	<b>1</b> F	<b>D1</b>	97	E1	95	ÂÂ	25	D2	CB	<b>E</b> 8	90	A1	53
DB       75       8F       9F       92       93       91       90       91       14       DA       53       30       51       30       1D       96         03       55       1D       0E       04       16       04       14       DA       27       4C       41       24       45       7B       02         D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06       03         55       1D       23       04       18       30       16       80       14       DA       27       4C       41       24       45       7B         02       D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06       03       30       01       01       FF       30       0D       01       01       01       01       01       01       03       02       03       03       01       01       FF       02       03       82       01       03       03       01		48	34	22	7D	<b>B8</b>	6F	<b>B3</b>	80	AA	çç	29	A8	<b>D</b> 2	9C	82	47
b3       35       10       b1       16       17       16       12       13       16       03         b5       10       23       04       18       30       16       80       14       DA       27       4C       41       24       45       7B         02       D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06         03       55       1D       13       01       01       FF       04       05       30       03       01       01       FF       30       0D       06       03       35       15       08       84       0D       61       00       03       82       01         01       00       3D       C9       31       35       35       58       88       40D       61       A0       25       C0       47         A8       56       EC       A3       A9       13       28       50       EE       2C       32       35       0F       33       C5       A7       42       B2       80       CC       90		<b>0</b> 3	55	8F 1 D	9F ØF	02 04	03 16	01 04	14	D1 D0	H3 27	53 40	30 41	51 24	30	1 U 7 R	ЮБ Ø2
55       1D       23       04       18       30       16       80       14       DA       27       4C       41       24       45       7B         02       D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       0F       06         03       55       1D       13       01       01       FF       04       05       30       03       01       01       FF       30       0D         06       09       2A       86       48       86       F7       0D       01       01       08       05       00       03       82       01         01       00       3D       C9       31       35       35       B8       84       0D       61       A0       25       C0       47         A8       56       EC       A3       A9       13       28       50       EE       2C       32       35       0F       33       C5         A9       32       42       74       4D       54       28       28       6A       C8       D7       4C		D8	58	ØΒ	õČ	13	ĒČ	74	F9	6E	FF	DF	ÂĒ	30	1F	06	<b>0</b> 3
02       D8       58       0B       6C       13       EC       74       F9       6E       FF       DF       AE       30       07       06         03       55       1D       13       01       01       FF       04       05       30       03       01       01       FF       30       0D         06       09       2A       86       48       86       F7       0D       01       01       08       05       00       03       82       01         01       03       DC       9       31       35       35       B8       84       0D       61       A0       25       C0       47         A8       56       EC       A3       A3       09       13       28       50       EE       2C       32       35       0F       33       C5         A9       32       42       74       4D       54       28       28       6A       C8       D7       4C       B2       80       CC       90         D0       A9       58       06       E6       A1       42       50       F7       36       F7		55	<b>1</b> D	23	04	18	30	16	80	14	DA	27	<b>4</b> C	41	24	45	7B
03       55       10       13       01       01       01       04       05       30       01 <td< td=""><th></th><td>02</td><td><b>D</b>8</td><td>58</td><td>ØB</td><td>6C</td><td>13</td><td>EC</td><td>74</td><td>F9</td><td>6E</td><td>FF</td><td>DF</td><td>AE</td><td>30</td><td>ØF</td><td><u>Ø6</u></td></td<>		02	<b>D</b> 8	58	ØB	6C	13	EC	74	F9	6E	FF	DF	AE	30	ØF	<u>Ø6</u>
01       00       3D       03       17       8D       8D       81       8D       6D       61       A0       25       C0       47         A8       56       EC       A3       A3       09       13       28       50       EE       2C       32       35       0F       33       C5         A9       32       42       74       4D       54       28       28       6A       C8       D7       4C       B2       80       CC       90         D0       A9       5B       06       E6       60       14       25       91       18       ED       E1       EF       31       42       1E         86       72       F2       4D       1B       9D       14       0C       6F       0C       96       DE       FF       D8       9E       85         D6       89       7E       49       A8       59       6A       8A       21       28       F7       36       15       10       E7       11         E3       78       48       4C       A2       30       BF       B4       93       F0       38		03 06	55	1D 20	13	01 49	01 86	ドド	04 Øn	05 01	30 01	03 Ир	01 05	01 00	FF Ø3	30	0 01
A8       56       EC       A3       A9       13       28       50       EE       2C       32       35       0F       33       C5         A9       32       42       74       4D       54       28       28       6A       C8       D7       4C       B2       80       CC       90         D0       A9       58       06       E6       60       14       25       91       18       ED       E1       EF       31       42       1E         86       72       F2       4D       18       9D       14       0C       6F       0C       96       DE       FF       D8       9E       85         D6       89       7E       49       A8       59       6A       A2       12       28       F7       36       15       10       E7       11         E3       78       48       4C       A2       30       BF       B4       93       F0       38       27       99       CE       D1       73         D6       42       FC       02       25       3C       F2       1F       BD       AA       32		01	ŏó	3D	Č9	31	35	35	85	B8	84	ЙĎ	61	ĂØ	25	čõ	47
A9       32       42       74       4D       54       28       28       6A       C8       D7       4C       B2       80       CC       90         D0       A9       5B       06       E6       60       14       25       91       18       ED       E1       EF       31       42       1E         86       72       F2       4D       1B       9D       14       0C       6F       0C       96       DE       FF       D8       9E       85         D6       89       7E       49       A8       59       6A       8A       21       28       F7       36       15       10       E7       11         E3       78       48       4C       A2       30       BF       B4       93       F0       38       27       99       CE       D1       73         DE       42       FC       02       25       3C       F2       1F       BD       AA       32       02       2F       EB       21       CB         78       C0       CF       C2       EE       84       E9       BF       EB       35		A8	56	EC	A3	A3	09	13	28	50	EE	2C	32	35	ØF	33	C5
D0       H7       SB       06       E6       b0       14       25       91       18       ED       E1       EF       31       42       1E         86       72       F2       4D       1B       9D       14       0C       6F       0C       96       DE       FF       D8       9E       85         D6       89       7E       49       A8       59       6A       8A       21       28       F7       36       15       10       E7       11         E3       78       48       4C       A2       30       BF       B4       93       F0       38       27       99       CE       D1       73         DE       42       FC       02       25       3C       F2       1F       BD       AA       32       02       2F       EB       21       CB         78       C0       CF       C2       EE       84       E9       BF       EB       35       AB       F4       C8       71       6C       23         E8       F5       61       E6       03       8C       2D       43       1C       0A		A9	32	42	74	4D	54	28	28	64		D7	4C	<u>B2</u>	80	CC	9Ø
bit       b		86	ну 72	5B F2	06 4 D	1 B	90 91	14	25 ЙС	6F	18 18	96 96	DE	FF	31 D8	42 9 F	85
E3       78       48       4C       A2       30       BF       B4       93       F0       38       27       99       CE       D1       73         DE       42       FC       02       25       3C       F2       1F       BD       AA       32       02       2F       EB       21       CB         78       C0       CF       C2       EE       84       E9       BF       EB       35       AB       F4       C8       71       6C       23         8       F5       61       E6       03       8C       2D       43       1C       0A       BF       E8       E1       99       E8       B2         93       A0       45       DA       58       15       ED       35       A2       0A       A1       E2       75       EE       EA       C8         8A       9F       B9       D0       46       D9       7A       76       44       FB       F1       FA       9B       AB       A8       79         DC       40       7F       15       8D       57       A7       0B       D4       30		D6	89	7Ē	49	<b>Ā</b> 8	59	ĜÂ	8Ă	21	28	F7	36	15	10	É7	11
DE       42       FC       02       25       3C       F2       1F       BD       AA       32       02       2F       EB       21       CB         78       CØ       CF       C2       EE       84       E9       BF       EB       35       AB       F4       C8       71       6C       23         F8       F5       61       E6       03       8C       2D       43       1C       ØA       BF       E8       E1       99       E8       B2         93       AØ       45       DA       58       15       ED       35       A2       ØA       A1       E2       75       EE       EA       C8         8A       9F       B9       DØ       46       D9       7A       76       44       FB       F1       FA       9B       AB       A8       79         DC       40       7F       15       8D       57       A7       ØB       D4       30       EB       2A       29       AE       F6       70         B2       F4       A3       61       5D       B8       6C       EØ       CD       FB		E3	78	48	4C	A2	30	BF	<b>B4</b>	23	FØ	38	27	99	CE	D1	73
78       C8       C1       C6       C2       L2       84       L7       Br       LB       53       HD       F4       C6       71       6C       23         E8       F5       61       E6       03       8C       2D       43       1C       ØA       BF       E8       E1       99       E8       B2         93       A0       45       DA       58       15       ED       35       A2       ØA       A1       E2       75       EE       EA       C8         8A       9F       B9       D0       46       D9       7A       76       44       FB       F1       FA       9B       AB       A8       79         DC       40       7F       15       8D       57       A7       ØB       D4       30       EB       2A       29       AE       F6       70         B2       F4       A3       61       5D       B8       6C       E0       CD       FB       51       96       7A       01       18       12         1C       3F       76       C4       84       D2       A8       9E       6F		DE	42	FC	Ø2	25	30	F2		BD	88 25	32	Ø2 24	2F	EB	21	CB
93       A0       45       DA       58       15       ED       35       A2       ØA       A1       E2       75       EE       EA       C8         8A       9F       B9       D0       46       D9       7A       76       44       FB       F1       FA       9B       AB       A8       79         DC       40       7F       15       8D       57       A7       ØB       D4       30       EB       2A       29       AE       F6       70         B2       F4       A3       61       5D       B8       6C       E0       CD       FB       51       96       7A       01       18       12         1C       3F       76       C4       84       D2       A8       9E       6F       65       FB       07       29       D9       24       C0         FD       10       E4       98       3A       B3       AB       B4       76       4D       C0       DE       44       00       4E       E1         37       62       00       00       A       AB       AB       AB       AB       AB	l	É	F5	61	E6	03	80	2D	43	10	ØÅ	BF	E8	E1	66	E8	B2
8A       9F       B9       D0       46       D9       7A       76       44       FB       F1       FA       9B       AB       A8       79         DC       40       7F       15       8D       57       A7       ØB       D4       30       EB       2A       29       AE       F6       70         B2       F4       A3       61       5D       B8       6C       E0       CD       FB       51       96       7A       01       18       12         1C       3F       76       C4       84       D2       A8       9E       6F       65       FB       07       29       D9       24       C0         FD       10       E4       98       3A       B3       AB       B4       76       4D       C0       DE       44       00       4E       E1         37       62       00       00       40       46       A       A       AB       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       <	l	93	ÂØ	45	DĂ	58	15	ED	35	A2	ØA	A1	E2	75	EE	EĂ	<b>C8</b>
DC       40       7F       15       8D       57       H7       0B       D4       30       EB       2H       29       AE       F6       70         B2       F4       A3       61       5D       B8       6C       E0       CD       FB       51       96       7A       01       18       12         1C       3F       76       C4       84       D2       A8       9E       6F       65       FB       07       29       D9       24       C0         FD       10       E4       98       3A       B3       AB       B4       76       4D       C0       DE       44       00       4E       E1         37       62       00       00       40       46       47	l	8A	9F	<b>B9</b>	DØ	46	D9	78	76	44	FB	F1	FA	9B	AB	<b>A8</b>	<b>79</b>
1C 3F 76 C4 84 D2 A8 9E 6F 65 FB 07 29 D9 24 C0 FD 10 E4 98 3A B3 AB B4 76 4D C0 DE 44 00 4E E1 37 62 00 00	l	DC 82	40 F4	7F	15	8D 5 D	57 P0	82	ØВ FØ	D4 CD	30 FP	EB 51	28	29	HE Ø1	F6 19	70
FD 10 E4 98 3A B3 AB B4 76 4D C0 DE 44 00 4E E1 37 62 00 00		10	3F	76	Č4	84	D2	<b>Å</b> 8	9E	6F	65	FB	07	29	D9	24	Ċΰ
37 62 00 00		FD	10	E4	98	3A	<b>B</b> 3	AB	<b>B4</b>	76	4D	CØ	DĒ	44	00	4E	E1
		37	62	00	90												

Figure 28 Serial console when showcert mode is enabled



D:\TLS1	ØGCo	demo	o\se	erve	er>o	oper	ารร]	L xs	509	-ir	n ce	ert	. per	n - c	out	form	der   hexdump -C
000000	30	82	03	53	30	82	02	Зb	a0	03	02	01	02	02	14	50	0S0;P
000010	10	dd	bc	f4	a8	Зc	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	g0*.H
000030	05	00	30	38	31	0b	30	09	06	03	55	04	06	13	02	54	081.0UT
000040	48	31	10	30	0e	06	03	55	04	08	0c	07	42	61	6e	67	H1.0UBang
000050	6b	6f	6b	31	17	30	15	06	03	55	04	0a	0c	0e	44	65	kok1.0UDe
0000000	73	69	67	66	20	47	61	74	65	77	61	79	30	20	17	Ød	sign Gateway0
000070	32	33	30	32	32	34	30	39	32	38	31	30	5a	18	0f	32	23022409281072
000070	31	32	33	30	31	33	31	30	39	32	38	31	30	5a	30	38	1230131092810708
0000000	31	Øb	30	89	06	63	55	94	96	13	92	54	48	31	10	30	1.0.U.TH1.0
0000000	80	96	93	55	94	88	80	97	42	61	60	67	6h	6f	6h	31	II Bangkok1
aaaaha	17	30	15	96	07 03	55	<b>6</b> 4	0a	80	0 <u>+</u>	<u>44</u>	65	73	69	67	66	0 II Design
ABBBCB	20	47	61	74	65	77	61	79	30	82	61	22	30	вd	96	69	Gatewave "e
aaaada	20 2a	86	48	86	<del>f</del> 7	øд	<u>61</u>	A1	A1	02 05	99	03	82	<b>6</b> 1	аf	66	* H
0000000	30	82	A1	00 Øa	A2	82	<u>61</u>	<u>61</u>	801	60	36	80	02 0a	dc	<u>4</u> f	hf	а <u>6</u> 0
aaaafa	90 Ah	102	10	30	77	17	of	hh	81	£3	25	a2	d2	f7	-T1 C2	69	<i>Асш</i>
000010	96	10	40	20	3-	ah	18	c1	87	fo	£3	h7	13	50	20	b6	жуш см. н.с.
000100	60		10	£⊿	21	bc	40	24	o/ oh	af	-F6	07 02	67	25	ha	02	
000110	5	90 6	24	14 6d	1 L	20	CZ d1	ou 24	ED		50	92 6h	0a 75	ਕਟ ੦-	وں جہ	95	
000120	50	20	24	12	10	70		24	07	21	29 66	00	75	21	10	00	(.4
000110	ee	ംപ	4a	74	00 مرد	72	90	20	97 47	21	60	14	⊃a ⊾o	22	40	94 	.oJ. r.#.!K.Z @.
000140	<u>ح</u> م	പ	20	24	4T	0/	04	20	a/	a⊤ ⊐o	22	17	10	90	eD 76	T/	c.+⊅0.060
000100	ат 2-	ot L	50	67	ze	eD	9/	42	64	/0	/ 2	1/	10	a4 70	70	/9	* AMU Ch
000170	Za	TD	5e	40	/5	00	C4	43	62	ba 7.c	c/	57	a9	72	e5	8e	*.^MUCDr
0001/0	/4	C5	ae	05	te	98	65	49	a3	/†	00	ae	39	31	9a	06	tel91
000180	38	ac	ta	ad	68	64	a0	3a ≎≎	69	51	a6	24	53	/c	81	6/	8nd.:.Q.\$S .g
000190	ta	ab	19	a9	að	95	34	99	/e	83	+1	68	6C	59	ca	49	4.~niY.i
000140	та	99	a/	34	4C	56	01	2a	83	aı	5C	12	CD	с8 75	83	40	4LV. <sup>+</sup> \K
000100	aa	53	58	11	66 -Ch	33	20	Ба	a2	49	1e	4e	59	/5	91	54	.SX3NYU.I
000140	/8	9a	85	3C		60	72	20	TT	aT Po	9/	eT	95	aa	25	a2	$X \dots ( \dots \Gamma 1 \dots \dots \hbar)$
000100	CD	eŏ	90	aı	53	48	34	29	7a	80	61	03	80	aa	cc	29	SH4)}.0)
000160	að	a5	90	82	47	ab	/5	8T	9T	62	03	01	66	91	as	53	S
000170	30	51	30	10	06	03	55	10	0e	04	16	04	14	da	2/	4C	
000200	41	24	45	70	02	að	58	90	6C	13	ec	74	†9	6e	++	at	A\$E{X.1t.n
000210	ae	30	11	00	03	55	10	23	04	18	30	10	80	14	da	2/	
000220	4C	41	24	45	70	02	a8 55	58	100	6C	13	ec	74	T9 05	6e	TT	LA\$E{X.1t.n.
000230	at	ae	30	UT 20	99	03	55	1a 2-	13	01	01		04	05	30	03	
000240	01	01	TT	30	0a	06	09	2a	86	48	86	T/	0a	61	01	90	
000250	05	66	25	82	47	-01	66	3a	c9	21	35	35	20	08	84	9a	- % C V (D
000260	61	ao	25	C0	47	að	56	ec	a≾	a≾	69	13	28	50	ee	20	a.%.G.V(P.,
000270	32	35	01	33	C5	a9	32	42	74	4a	54	28	28	6a	60	a/	25.32BtMI((]
000280	4C	b2	80	cc	90	a0	a9	50	06	e6	60	14	25	91	18	ea	L[
000290	eı	et	31	42	1e	86	/2	+2	4a	10	9a	14	90	61	90	96	1Br.Mo
0002a0	ae	tt 4E	a8	9e	85	a6	89	/e	49	að	59	6a	8a	21	28	†/	
000200	36	15	10	e/	11	e⇒	/8	48	4c	a2	30	D†	04	93	<del>1</del> 0	38	6XHL.08
000200	2/	99	ce	a1	/3	ae	42	tc	62	25	30	+2	1+	ъа	aa	32	·
0002d0	02	2†	eb	21	cb	/8	C0	C†	c2	ee	84	e9	b†	eb	35	ab	./.!.X5.
0002e0	+4	c8	71	6C	23	e8	+5	61	e6	03	80	2d	43	10	0a	b†	ql#aC
0002+0	eð	e1	99	eð	62	93	a0	45	da	58	15	ed	35	a2	0a	al	E.X5
000300	e2	75	ee	ea	c8	8a	9†	b9	d0	46	a9	/a	76	44	†b	+1	.uF.zvD
000310	ta	96	ab	a8	79	ac	40	/†	15	8d	57	a/	06	d4	30	eb	y.@W0.
000320	2a	29	ae	<del>1</del> 6	70	b2	+4	a3	61	5d	68	60	e0	cd	†b	51	*)pa].lQ
000330	96	7a	01	18	12	1c	31	76	c4	84	d2	a8	9e	6 <del>1</del>	65	†b	.z?voe.
000340	07	29	d9	24	c0	†d	10	e4	98	За	b3	ab	b4	76	4d	c0	.).\$VM.
000350	de	44	00	4e	e1	37	62										.D.N.7b

Figure 29 Certificate information from openssl command



#### 8.7 Download data

command> myGET protocol://ip:port/download/pattern/length

This command simulates GET method of HTTP to download data from the server. Users can input a URL and then received data is displayed on the serial console. For download data pattern, the verification feature is enabled. If the received data matches the expected data, the total length of received data and download speed are displayed on the serial console.

In case of the downloaded data length exceeds 16kB, "Data Length is too large, Show only Transfer speed" is displayed instead of the received data, as shown in Figure 30.



Figure 30 Serial console when downloading large data

Serial console when downloading large dataIn this demonstration, the maximum data length is limited at 2 GB for testing with the test software and 1 GB for testing with serverDemo.js, respectively. When users request to download data exceeding the maximum length, an error message is sent from server, causing the verification to fail, and the actual data and expected data will be displayed on the serial console.

For downloading HTML page, the verification feature is disabled. The received data is displayed on the serial console, as shown in Figure 31.







## 8.8 Upload data

command> myPOST protocol://ip:port/upload/pattern/length

This command simulates POST method of HTTP to upload data to the server. Users can specify the data pattern and data length in the URL. After the upload is completed, the data length and upload speed are displayed, as shown in Figure 32 and Figure 33. On the server's console, the number of data sent from the client and transfer speed is displayed. If the data length is less than 16 kB, the received data is also displayed, as shown in Figure 34.



Figure 32 Serial console when uploading large data



Figure 34 Server console when uploading 123-byte data

## 8.9 Full duplex test

command> myFullduplex protocol://ip:port/fullduplex/pattern/length

This command is used to transfer data between the client and server in full duplex mode. It simulates POST method of HTTP with the fullduplex URL, which requests a data pattern from the server and uploads the data pattern to the server. Users can specify the data pattern and data length in the URL. After the transmission and reception of data are complete, the data length and transfer speed are displayed, as shown in Figure 35.



Figure 35 Serial console when full duplex mode is tested



## 9 Test setup when using 2 FPGA boards

## 9.1 Environment setup when using 2 FPGA boards

To operate TLS10GC-IP demo with TLS10GS-IP demo, please prepare following test environment.

- 1) FPGA development boards (ZCU106 as a client and ZCU102 as a server).
- 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 ZCU102 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 TLS10GCIPTest.bat" and TLS10GSIPTest.bat" (To download these files, please visit our web site at www.design-gateway.com)



Figure 36 TLS10GC-IP demo environment when using 2 FPGA boards

Follow step 1)-8) of Topic 6 Board Setup to prepare FPGA boards for running the demo. Run "TLS10GCTest.bat" to download configuration file and firmware to ZCU106 board as a client and run "TLS10GSTest.bat" to download configuration file and firmware to ZCU102 board as a server. The details of supported commands and their usage for TLS10GC-IP demo is described in the following link.

https://www.dgway.com/products/IP/TLS-IP/TLS10GSIP-instruction-xilinx-en/



#### 9.2 Test sequence

#### 9.2.1 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 a server, as shown in Figure 37 by entering the following command in server's console:

#### listenFor <client's IP address> on <server's port number>

TLS10GS	TLS10GC
TLS10CS version 0x80011C40	TLS10GC version 0x80011841
<pre>Usage: [1] setip ddd.ddd.ddd Set FPGA's IP address in dotted-decimal format. [2] setmac hh-ph-hh-ph-hh Set FPGA's MC address in hexadecimal format. [3] showkey (1: enable, 0: disable&gt; Enable showkey mode for show ILS traffic ticket, session key and iv for encryption/decryption. [4] setcert w file via serial console. [5] setrekey Set server's RSA key infomation by inputing ASN.1 DER Certificate in bin ary file via serial console. [6] listenFor ddd.ddd.ddd.odd on ddddd Larve a server to listen for specified client's IP address in dot ted-dccimal format on specified server's port in decimal format. To terminate the process, please press Ctrl+C. &gt;&gt; setip 192.168.7.25 Set FPGA's IP Address to 000-11-22-33-44-55 &gt;&gt; setcert *** Fill Certificate *** send file over serial console Complete! &gt;&gt; setrakey *** Fill RSA private key *** end file RSA private key *** end file RSA private key ***</pre>	Usage: [1] setip ddd.ddd.ddd Set PFGM's IP address in dotted-decimal format. [2] setport ddddd Set PFGM's aport number in decimal format or type dynamic/d/-d to set dynamic port number. [3] setmac hip-hh-hip-hh- [4] showkey (1: enable, 8: disable) [4] showkey (1: enable, 8: disable) [5] showcert (1: enable, 8: disable) [6] myGET https://download.pattern/length Send GET command for download.ing pattern data from server. [7] myPOSI https://ip:port/ubload/pattern/length Send GET command for uploading pattern data to server. [8] myFullduplex https://jp:port/ubload.pattern/length Test fullduplex with test software. [3] showcert 5: 18.7.42 Set FFGM's 1P Address to 99-81-82-83-84-85 [3] setport 60800 Set Port number to 60808 >> []
Complete >> listenFor 192.168.7.42 on 60001	
Server listening on 192.168.7.42 port 60001 Wait Open connection	

Figure 37 Server and client console when parameters are set

#### 9.2.2 Transmit data test (Server to client)

Enter the command myGET protocol://ip:port/download/pattern/length through client's console to request the data pattern from TLS10GS demo. Once the data transfer is complete, the transfer results and speed will be presented on both client's and server's consoles, as shown in Figure 38.



Figure 38 Server and client console when transfer data from server to client



## 9.2.3 Receive data test (Client to server)

Enter the command myPOST protocol://ip:port/upload/pattern/length through client's console to transmit the data pattern from TLS10GC demo to TLS10GS demo. Once the data transfer is complete, the transfer results and speed will be presented on both client's and server's consoles, as shown in Figure 39.





## 9.2.4 Full duplex test

Enter the command myFullduplex protocol://ip:port/fullduplex/pattern/length through client's console to test transfer data in full duplex mode between TLS10GS demo and TLS10GC demo. Once the data transfer is complete, the transfer results and speed will be presented on both client's and server's consoles, as shown in Figure 40.



Figure 40 Server and client console when transfer data in full duplex mode



## 10 Test results

This demonstration, TLS10GCdemo is showcased for its ability to function as a secure client. The HTTPS protocol is chosen as the application layer to demonstrate that TLS10GC-IP can implement TLS1.3 to secure HTTP communication. The subsequent section details the test results when transferring data between each component, covering 2 main aspects: functionality testing and performance testing.

## **10.1 Functionality testing**

TLS10GCdemo is designed to send HTTPS request to a server, demonstrating that TLS10GC-IP can handle TLS1.3 connection similar to a web browser. As shown in Figure 41 and Figure 42, a web browser requests a data pattern via the GET command and displays the received HTTP payload from the server on the browser, producing the same result on the serial console of TLS10GCdemo.



Figure 41 Test results when web browser download data from node.js server



Figure 42 Test results when TLS10GCdemo download data from node.js server



#### TLS10GC IP Core

In the case of uploading data, TLS10GCdemo is capable of transmitting a data pattern with HTTP header to the server. The receiving results shown on the server console upon completing the reception of data from TLS10GCdemo, as shown as Figure 43, are similar to when receiving data from a web browser, as shown as Figure 44.

Node.js server				Browser	
C:\Windows\System32\cmd.exe - node serverDemo.js			×	✓	×
 0000000100			^	← → C ③ File file:///D:/36.TLS ☆ ♪ □ ▲	:
Received data length = 5 byte(s). Transfer speed: 0.24 Mbps.				Upload menu	^
				choose your data pattern.	
				DataPattern : Increasing v binary v	
				DataLength : 5 byte(s)	
				POST	
				Increasing binary pattern 5 byte(s) is uploaded!	*
Figure 43 Test resu	lts wh	en we	b br	owser upload data to node.js server	



Figure 44 Test results when TLS10GCdemo upload data to node.js server

#### **10.2 Performance testing**

When the example node.js server is used as a server to communicate with TLS10GCdemo, the CPU manages encryption/decryption during data transfer, causing a decrease in transfer speed. To achieve the maximum throughput, the "server" application is used instead.

"Server" application is designed to encrypt data before transmission through the network in Tx mode, decrypt the last data block and verify the total received data size only in Rx mode. As shown in Figure 45 and Figure 46, the transfer speed is nearly by 10 Gbps and the utilization of the Intel i7 CPU is approximately 100%, as monitored by the PC's task manager. This indicates that if the CPU is tasked with encrypting/decrypting data while transferring data through the network, the transfer speed will be reduced.

"server" application		TLS10GC	
Client download length Generate Data: 2147483 Transmitted data: 2147 Thoughtput 9100.27 Mbp	n : 2147483647 Byte 8647 Byte Success! 7483647 Byte Success! os	<pre>&gt;&gt; myGET https://192.164 Open connection Connected from 192.168. Downloading Data Length is too large Close connection Connection is closed. Received data length = 2 Download Speed 9008 Mbps</pre>	8.7.26:60001/download/t1/2147483647 7.26 e. Show only Transfer speed 2147483647 Byte <s></s>

Figure 45 Test results when TLS10GCdemo upload data to node.js server



Figure 46 Test results when TLS10GCdemo upload data to "server" application



#### TLS10GC IP Core

For full duplex mode, the transfer speed between "server" application and TLS10GCdemo decreases, as shown in Figure 47. This suggests that the CPU cannot handle both receiving and transmitting task in a secure connection to maintain the 10 Gbps throughput.

In the testing scenario between two FPGA boards, where TLS10GCdemo acts as a client and TLS10GSdemo as a server, cryptographic tasks, including encryption/decryption, are entirely offloaded to hardware. As shown in Figure 48, the throughput increases to 9360 Mbps, representing the maximum throughput achievable with TCP/IP in this demonstration.



Figure 47 Full duplex test results between TLS10GCdemo and "server" application



Figure 48 Full duplex test results between TLS10GSdemo and TLS10GCdemo



## 11 Revision History

Revision	Date (D-M-Y)	Description
1.03	2-Apr-25	Add setgatewayip command
1.02	5-Mar-24	Add test results between 2 FPGA boards
1.01	22-Dec-23	Add full duplex test
1.00	8-Sep-23	Initial version release