Instructions for DNP3 Over Ethernet

V1

Created By:	Edwin Wright	Date:	August 2014
Reviewed By:	Robert Holm	Date:	Sept 2015

ENGINEERING INSTITUTE OF TECHNOLOGY

DNP 3.0 Over Ethernet

<u>Aim:</u> To demonstrate the use of a Remote Telemetry Unit (RTU) in the transfer of control messages over Ethernet using the DNP 3.0 protocol. The ScadaSoft DNP Demon Lite is used as a Master to generate DNP3 messages sent to a DATRAN XL4 DNP3 RTU. These messages are viewed on the Master and captured on the LAN segment by the Wireshark protocol analyzer for viewing and analysis.

Equipment on Server:

DNP Master Simulator - ScadaSoft DNP Demon Lite DATRAN XL4 DNP3 RTU Wireshark Protocol Analyzer Ethernet LAN

Student Software Required:

Screen capture software such as ScreenHunter

Method Part 1 - Configuration and Data Capture

Log onto the Electromeet lab environment in the usual manner

Select Remote Lab 2

Locate the DNP Demon Lite icon on the desktop . Open it by double clicking on the icon.

The following screen will open :-

le View Advan	ced Help				a	
Set-Up DNP Address	Form 6 IP Address	Transport	Timinas Auto Polling every 500 ms	IIN Bits 📕		RX]
Device 2	192 168 1 50 • TCP/IP Remote Port	- Pollings - Catrl-	Wait for Response 3000 ms Keep Alive	All stations Class 1 avail	DigOut Local Trouble	Invalid par Event OV
Device	C UDP/IP 20000	a oning calu	Link Confirm	Class 2 avail	Restart	Already Ex
	Courses Listen Discourses		14 Obb Continu	Class 3 avail	Unsupported	Corrupt Cf
	Connect Listen Disconnect			Time supe	Obiupkpown	Receiver

e view Auv	anced Help			
Set-Up DNP Address Remote Device 2	Form 6 IP Address	- IP Serial R	Auto Polling every 500 ms sit for sponse 3000 ms	CP Connected TX RX
This Device 1	Connect Listen Discon	Polling Cntrl	Keep Alive Link Confirm App Confirm Class 2 avail Class 3 avail Time sync	Trouble Event 0 Restart Already Ex Unsupported Corrupt 0 Obj unknown Reserved
DNP Communic	ations		117	
Timo	Data	ITranclati		
The	Data	11 di Stach	JE I	
		- IS		
		19 19		
		8 		
4				

Click "Connect" and the following screen opens : -

We will now prepare the Wireshark Protocol Analyzer to observe the DNP3 packets as they traverse the network to and from the RTU. Open Wireshark by double-clicking on the icon as shown to the right.



Next, we must start a 'capture session' with Wireshark, and then generate some DNP3 traffic across the network. To start a capture session, simply click on the link for the *Intel(R)* 82579LM Gigabit Network Connection interface:'

The screen will change and start displaying the data for packets as they are seen at the network interface. To get Wireshark to only display the DNP3 protocol packets (the ones we are interested in), simply enter **dnp3** into the filter box as shown below and then press the 'Apply' button. The capture screen should now go blank since there will be no dnp3 messages yet.

Captu	iring from	Intel	(R) 8257	79LM (Gigabit	Netwo	ork Cor	nnecti	ion - \	Viresh	ark							
<u>F</u> ile <u>E</u> di	t <u>V</u> iew	Go	<u>C</u> aptu	ire <u>A</u>	Analyze	Stat	istics	Tele	phony	<u> </u>	ols	He	lp					
	S				× 2		10	4		\$	Ŧ	₽			Ð	Q	Q	
Filter: dr	прЗ											٠	Expression	h	Clea	(App	oly]	
No	Time						Sour	rce					Destina	tion	0			

Switch back to the **DNP3 Demon Lite** using the icon on the task bar at the foot of the screen and maximise the DNP3 Demon window.

Now click on the "Polling " icon

-	-	
C	2	
-	-	н

The "Send Commands "window then opens

Polling	Unsolicited
Static Poll	Enable Unsolicited
Event Poll	
Integrity Poll	Disable Unsolicited
Clear Restart	Delay Measurement
Reset Link	Time Synch
Link Status	Read Time
Freeze Counters	Freeze Analog Inputs

Now click on "Reset Link" and observe the DNP3 command message (shown in green) and the response message (shown in red) in the DNP Communications window as shown.

Time	Data	Translation
05:01:49.05 >	05 64 05 C0 02 00 01 00 9E 59	Destination TCP/IP Address 192.168.1.50:20000 sent from Local Port 49757 Datalink Header Request RESET Link Destination = 2 Source = 1
05:01:49.08 <	05 64 05 00 01 00 02 00 BA	Source TCP/IP Address 192.168.1.50:20000 received on Local Port 49757 Datalink Header Response ACK Destination = 1 Source = 2

Swap back to Wireshark and you will see the two captured DNP3 messages. Select the "Reset of Remote Link " message. Expand all the "+ " tabs for the DNP message and rearrange the windows so you can see all of the DNP details as well as the bytes in the bottom window. Capture this in one screenshot and attach to your document as **SCREENSHOT 1**.

Return to the DNP Demon and click on "Time Synch" and similarly observe the messages in Wireshark. Select the message "DNP 3.0 Write" and expand the DNP, Application Layer and all the Write Request Data Object tabs. Then rearrange the windows so you can capture the decoded frame as well as the data bytes. Take a screenshot attach this to your document as **SCREENSHOT 2**.

Now return to the DNP Demon and click on "Integrity Poll". After a while it will generate several messages.

Swap to Wireshark and select the message " DNP 3.0 Read, Class 0123" Expand all the DNP, Application Layer and the READ Request Data Objects tabs. Then rearrange the windows so you can capture the decoded frame as well as the data bytes. Take a screenshot and attach this to your document as **SCREENSHOT 3**.

Now select the "DNP3.0 Confirm" message in Wireshark and expand the DNP3 and all the Application Layer tabs. Then rearrange the windows so you can capture the decoded frame as well as the data bytes. Take a screenshot and attach this to your document as **SCREENSHOT 4**.

Now close down the lab session, simply exit Wireshark and "Quit without Saving"

Then return to the DNP Demon and click on the "Disconnect " button

Set-Up DNP Address	Form 6 IP Address	Transport	Timinas Auto Polling every 500 ms	IIN Bits	TCR Closed	TX 🔜 🦉
Device 2 This 1	[192] 168] 1] 50 [CP/IP Remote Port [C UDP/IP 20000	Polling	Wait for Response 3000 ms Keep Alive Link Confirm	All stations	DigOut Local Trouble	Invalid parm
Device 1	Connect Listen	i 🗵 🗉	App Confirm	Class 3 avail	Unsupported	Corrupt Cfg

Now Log off the server (Do not save any files on server).