Instructions for DNP3 Over Ethernet

V1

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

EIT ENGINEERING INSTITUTE OF TECHNOLOGY

DNP 3.0 Over Ethernet

Aim: 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

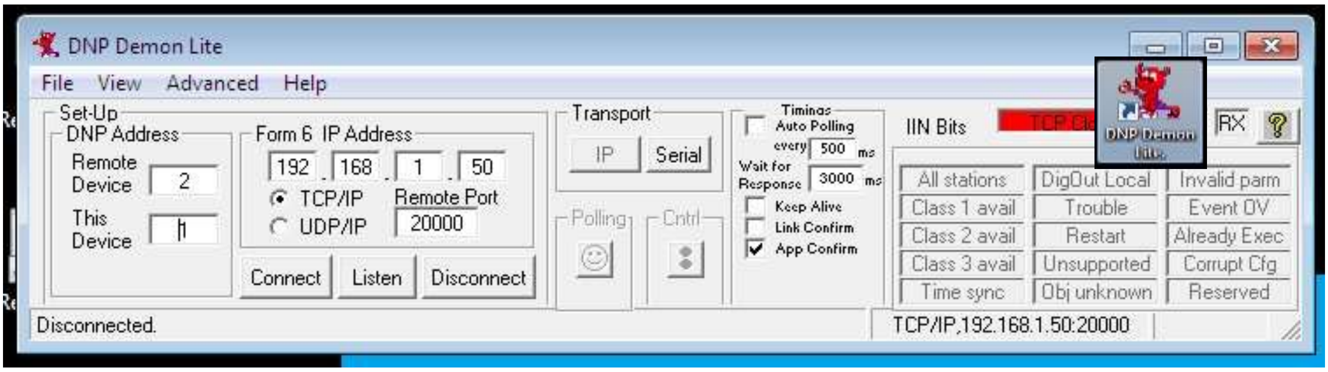
Part 1 - Configuration and Data Capture

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.

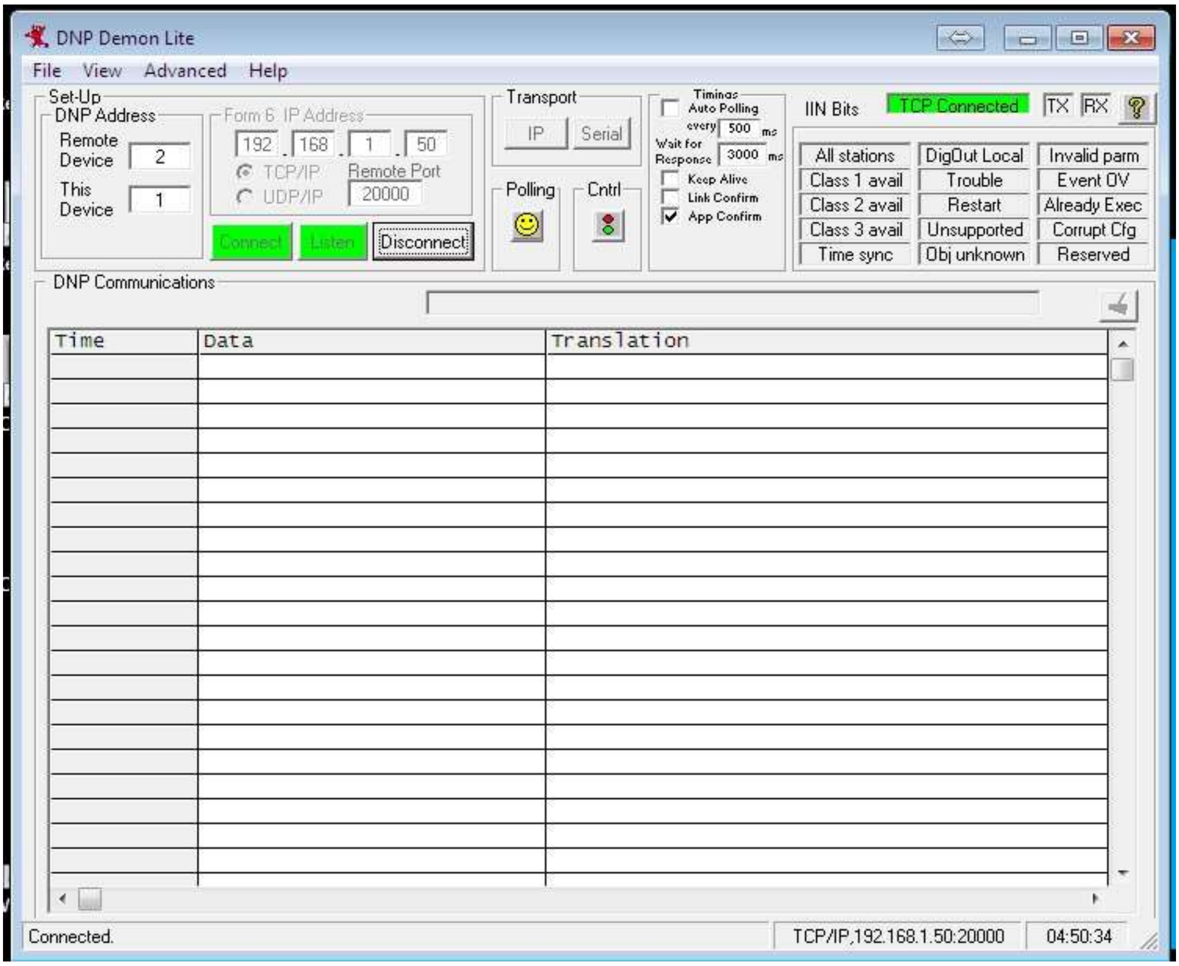
The following screen will open :-



Remote Device 2
This Device 1
Form 6 IP Address 192 . 168 . 1 . 50
● TCP/IP ○ UDP/IP
Remote Port 20000
□ Auto Polling every 500 ms
Wait for Response 3000 ms
□ Keep Alive
□ Link Confirm
☑ App Confirm

Disconnected.
TCP/IP,192.168.1.50:20000

Click “Connect” and the following screen opens : -



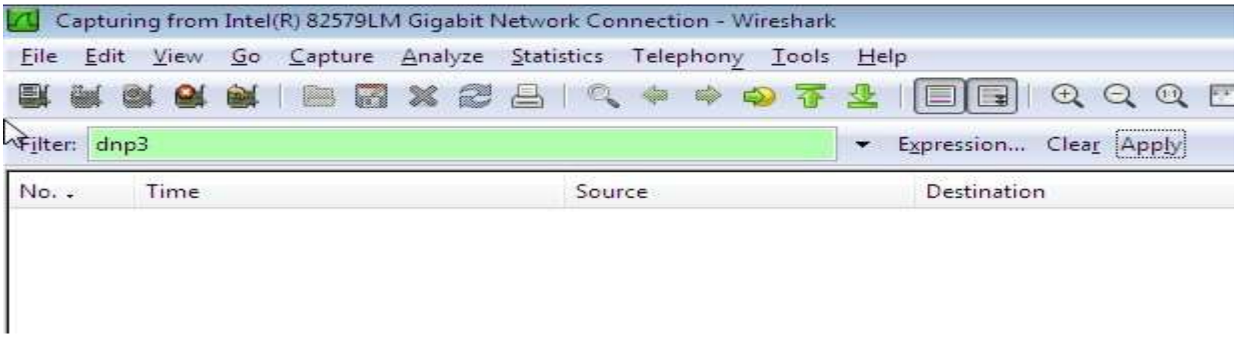
Remote Device 2
This Device 1
IP Address 192 . 168 . 1 . 50
● TCP/IP ○ UDP/IP
Remote Port 20000
□ Auto Polling every 500 ms
Wait for Response 3000 ms
□ Keep Alive
□ Link Confirm
☑ App Confirm

Connected. | TCP/IP,192.168.1.50:20000 | 04:50:34

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:’

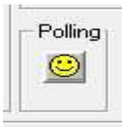
The screen will change and start displaying the data for packets as they are seen at the network interface. To get Wireshark to only display the DNP3 protocol packets (the ones we are interested in), simply enter **dnp3** into the filter box as shown below and then press the ‘Apply’ button.   The capture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


Capturing from Intel(R) 82579LM Gigabit Network Connection - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
No. Time Source Destination

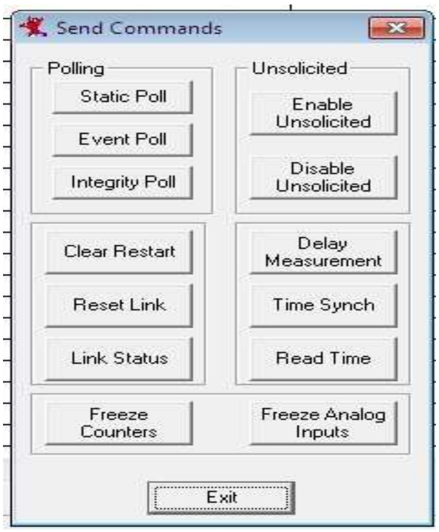
Filter: dnp3

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.

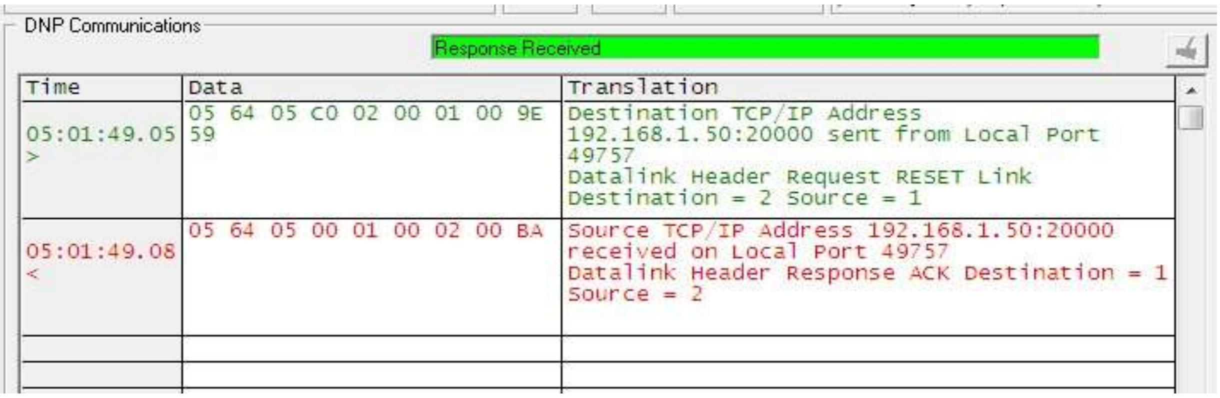
Now click on the "Polling " icon



The "Send Commands "window then opens



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**.

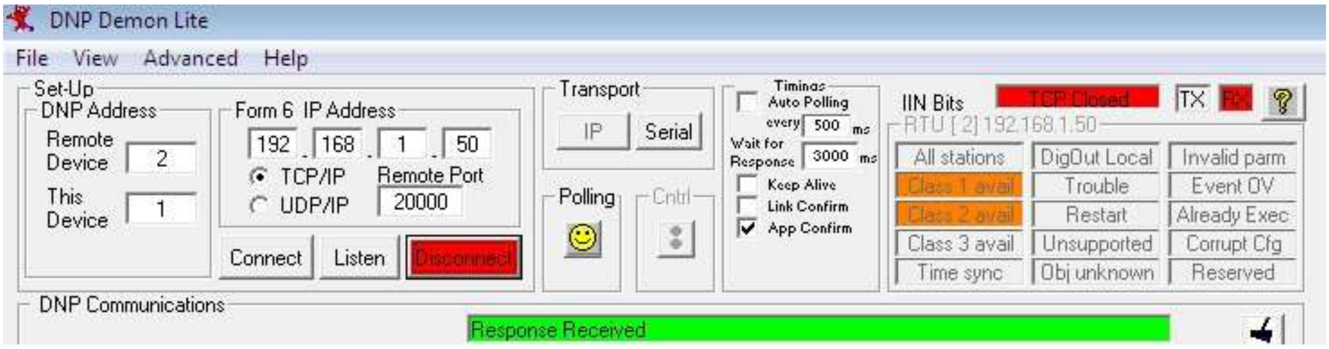
Now return to the DNP Demon and click on " Integrity Poll" . After a while it will generate several messages.

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



Remote Device 2

This Device 1

IP Address 192 . 168 . 1 . 50

● TCP/IP ○ UDP/IP

Remote Port 20000

□ Auto Polling every 500 ms

Wait for Response 3000 ms

□ Keep Alive

□ Link Confirm

☑ App Confirm

TCP Closed

RTU [2] 192.168.1.50

Response Received

<span style="color:red">Now Log off the server (Do not save any files on server).</span>