Configuring SCADAPack E RTUs with Dynamic IP Addressing for Use in Cellular IP Networks

December 2013 / Technical Note

Make the most of your energy

Schneider Electric

Using SCADAPack E RTUs with Dynamic IP Addressing

Purpose

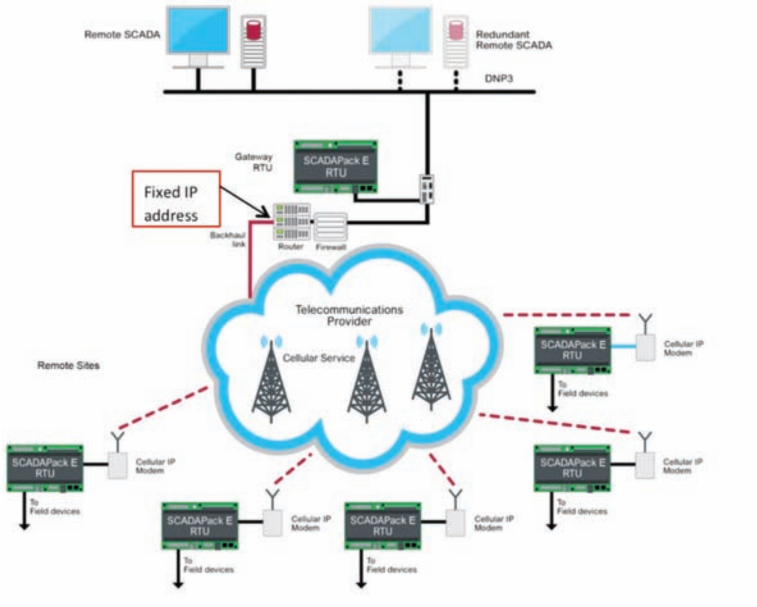
The purpose of this document is to outline a system configuration in which a master station is able to communicate with SCADAPack E RTUs using DNP3 protocol over TCP/IP in an environment where the remote communication devices receive their IP addresses in a dynamic fashion; i.e. where the remote link does not have a static IP address as seen by the master station (host) network. This situation commonly occurs when using cellular IP infrastructure, such as GPRS, as a remote communication network.

A key part of this architecture is the use of a Gateway RTU at the master station (host) to resolve DNP3 addresses with dynamic IP addresses.

Requirements

There are several requirements / specifications which must be met to successfully implement the architecture presented in this document:

- DNP3 master station (host) or other DNP3 master device, should be Level 2 Conformant (or higher). ClearSCADA is used as an example in this document. Other masters may be used
- When using a SCADAPack 300E as the Gateway RTU it is not recommended to exceed 25 remote RTUs
- When using a SCADAPack ES as the Gateway RTU it is not recommended to exceed 90 remote RTUs
- The minimum SCADAPack E firmware version required is 8.05 in all devices
- One fixed IP address is required from the telecommunications provider as the contact point for the Master Station (Host system)
- TCP transport must be used between all remote RTUs and the Gateway RTU



• Figure 1: System Architecture for dynamic IP addressing management using DNP3

Background: SCADAPack E DNP3 Routing Mechanisms

The solution to using dynamic IP addresses with DNP3 primarily lies in the understanding of how to configure the DNP3 routing mechanism provided by the SCADAPack E RTU.

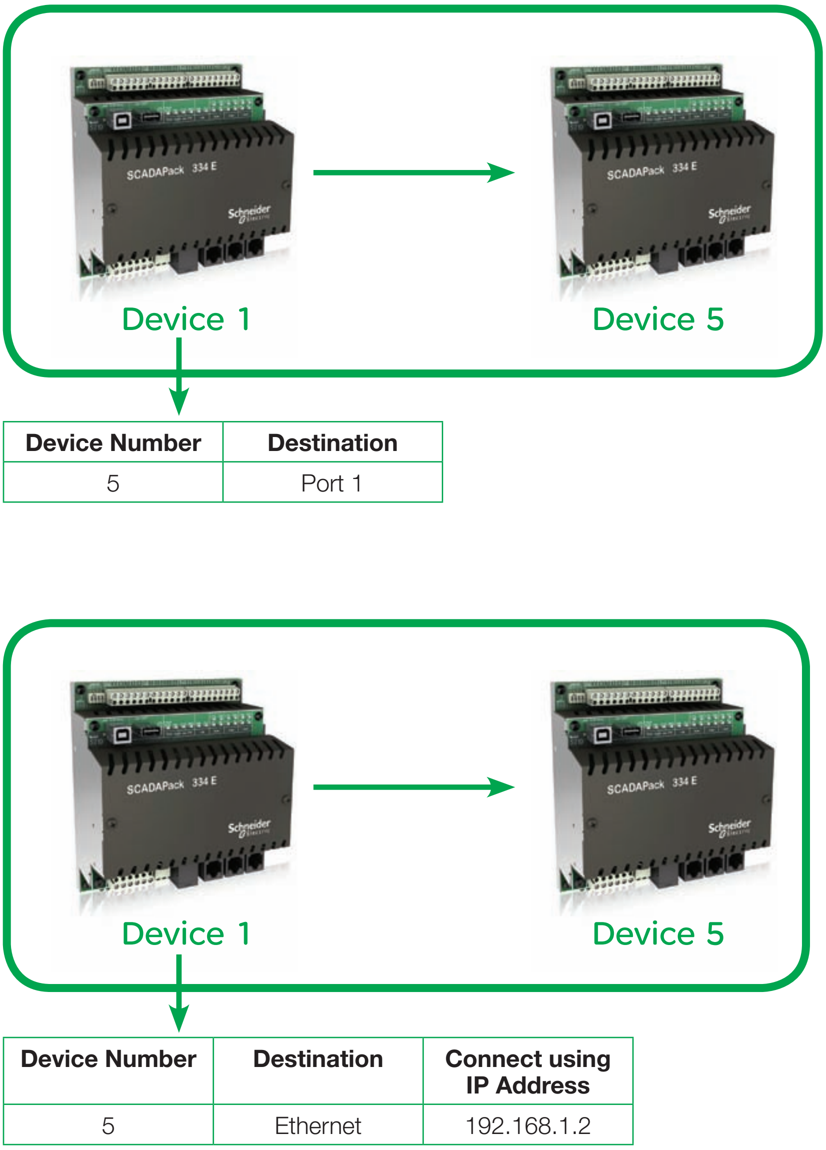
In the examples shown in Figure 2 we will use DNP3 device 1 and device 5 to illustrate SCADAPack E routing.

Device 1 will be a SCADAPack E RTU configured for routing. (In the architecture and configurations presented below we will refer to this as a *Gateway RTU*). Device 5 will be the remote RTU we are trying to communicate to.

The configuration of a SCADAPack E includes a table for DNP3 device addresses and their associated routing paths in relation to itself. For example, you can add an entry in the routing table in device 1 which tells it that device 5 may be reached across a network connected to serial port 1. If device 1 needs to send a message to device 5 it will check the routing table entries and discover that device 5 may be reached through serial port 1. It will then send the message out on serial port 1.

This routing mechanism works the same way for an Ethernet port with the added requirement of an IP address associated with the DNP3 address. As in the previous example, if device 1 needs to send a message to device 5 it will check the routing table, discover that DNP3 address 5 is on the Ethernet port and will then send the message out the Ethernet port to the IP address it finds in the routing table.

SCADAPack E routing also applies to external traffic received by the RTU. When receiving a DNP3 message which is not bound for the RTU, it will search the routing table and forward that message if a relevant route is found.



Device Number	Destination
5	Port 1

Device Number	Destination	Connect using IP Address
5	Ethernet	192.168.1.2

• Figure 2: Basic serial and Ethernet SCADAPack E DNP3 Routing entries

As an example, if our device 1 receives a message on serial port 3 from device 30000, which is bound for device 5, it can forward that message out serial port 1 to device 5. A received response from device 5 (to the previously routed message from device 30000) will follow the reverse path and be routed from serial port 1 to the requester on serial port 3 (see Figure 3).

Now that the routing table operation has been discussed, the mechanism for how to solve the dynamic IP addressing problem will be introduced.

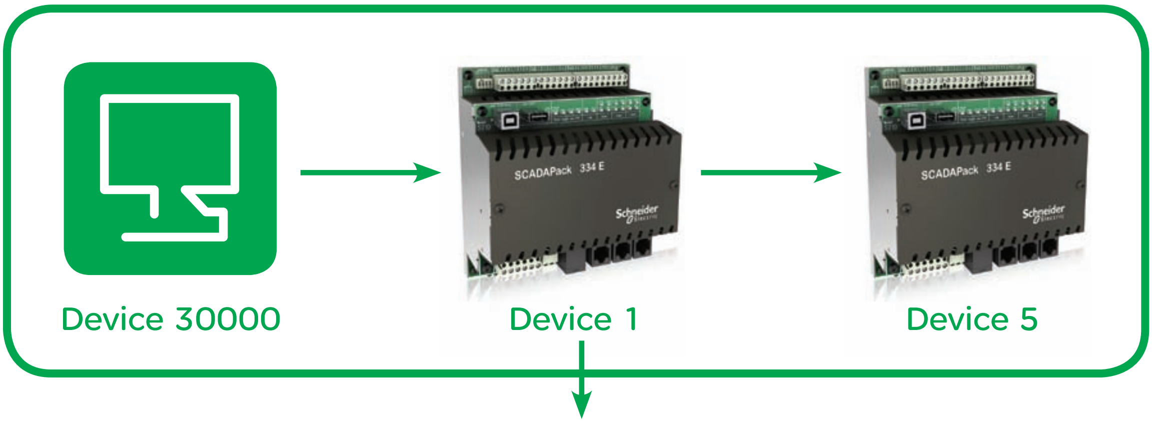
The solution to the problem of a changing IP address at a remote device lies in the DNP3 routing tables' ability to update routes online, meaning that the SCADAPack E RTU may build and update routing table entries on its own. (This behaviour can be disabled through configuration if necessary). Please refer to the SCADAPack E Reference documentation for more information on DNP3 routing tables. The routing table entries are created or updated when a communication path has been established to a DNP3 device. For example, if a routing table entry is created in our device 1 for DNP3 device 5 which states that it is located on serial port 1 but subsequently device 1 discovers that device 5 is actually connected to serial port 2 it will update its entry in the routing table, and thereafter use serial port 2 for communication with device 5.

As before, this also works on an Ethernet interface, so if a route entry for device 5 has, for example, IP address 192.168.1.2 configured but the next message coming from device 5 is received with a different IP address (say 192.168.1.5), that entry in device 1's routing table will be updated. Thereafter device 1 will send messages for device 1 to its actual IP address at 192.168.1.5.

The online updating of the routing table is performed by a SCADAPack E when any DNP3 message is received. If a device already has an existing entry in the routing table then it is updated with the port and IP information from the received message. Make sure entries are created for all known remote RTUs (If there is no matching entry in the routing table, a Dynamic route is created for communication with that device. This should be avoided in most cases as dynamic route entries expire).

The most common conditions under which an "On Static" route entry is updated (on receiving a message from a port or IP address that is different from that configured in the routing table entry):

- RTU receives a response to a request
- RTU receives an unsolicited message from a device
- RTU receives a DNP3 data link status message (also known as a keep-alive message)



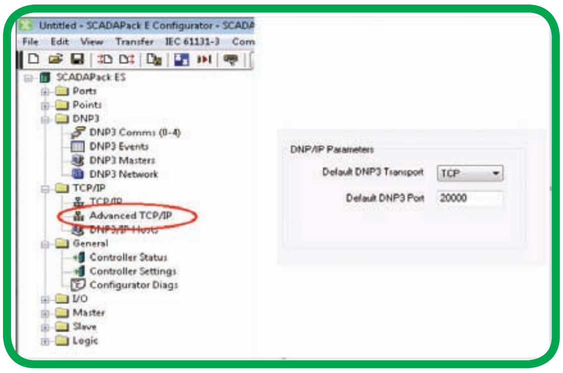
Device Number	Destination
5	Port 1 →
← 30000	Port 3

• Figure 3: SCADAPack E DNP3 Routing

System Architecture

To configure a system in which the remote RTUs will use dynamic IP addressing (for example coming from a GPRS network) we will make extensive use of the principals outlined above; DNP3 route entries will be updated automatically online and be used to route DNP3 messages from the host (master station) to the remote RTUs.

For the host to be unaffected by the dynamic IP addresses of the remote RTUs, the architecture in Figure 1 should be used:



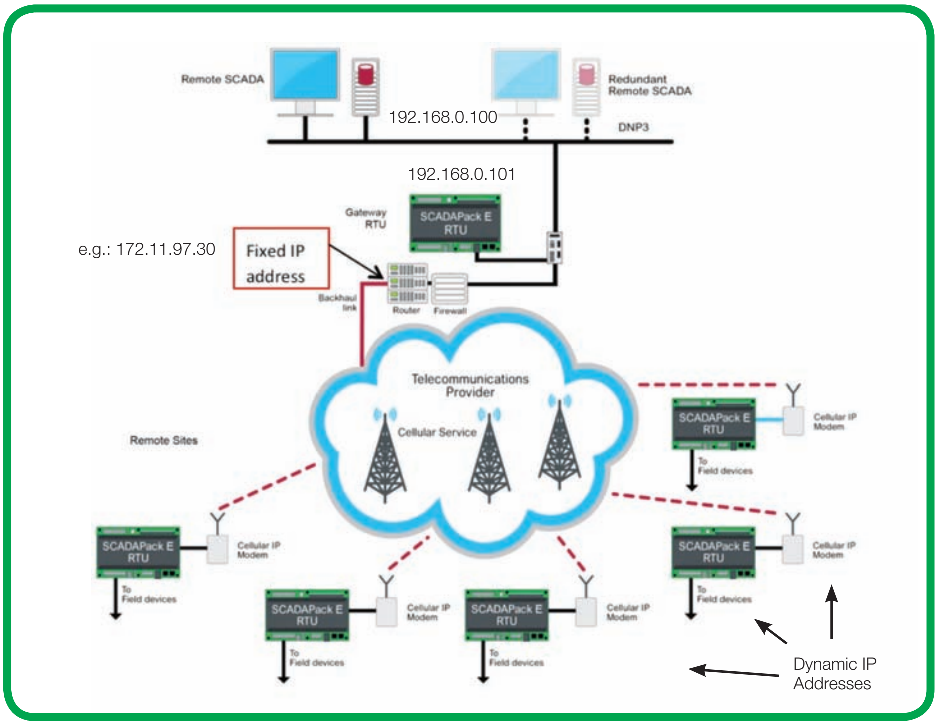
DNP/IP Parameters

Default DNP3 Transport: TCP

Default DNP3 Port: 20000

• Figure 4: Changing the Default DNP3 Transport

- The host will send all of its DNP3 traffic through a local Gateway RTU
- The Gateway RTU and all remote RTUs must have their Default DNP3 Transport set to “TCP” (see Figure 4)
- The Gateway RTU will be responsible for maintaining the routing table containing the remote RTU DNP3 addresses and their associated IP addresses. When a DNP3 message for a specific remote RTU arrives at the gateway (e.g. from the host) it will forward that message on, using the appropriate IP address, to the remote RTU. Responses received from the remote RTU will be forwarded back to the host
- Each remote RTU must use the DNP3 TCP Keep-Alive feature to keep its connection with the Gateway RTU established and to keep the routing table in the Gateway RTU updated. This is a vital part of the operation of this architecture, as without this keep-alive message the gateway would not be updated with the changing IP address of each remote RTU



• Figure 5: Example IP addressing for dynamic IP management using DNP3

Network Infrastructure Configuration

In order for this architecture to work it is very important to configure the IP network infrastructure properly. DNP3 eases this through the use of a single IP port number for establishing connections between devices, which is port 20000 by default. If there are any routers, firewalls, IP gateways or other devices involved in the IP infrastructure, these devices will need to be configured to allow access via port 20000 into and out of the network.

It is important to understand how all the devices will interact with the network in terms of the IP addresses. On the internal network, where the gateway and host are located, there will be a set of IP addresses in use, for example 192.168.1.x.

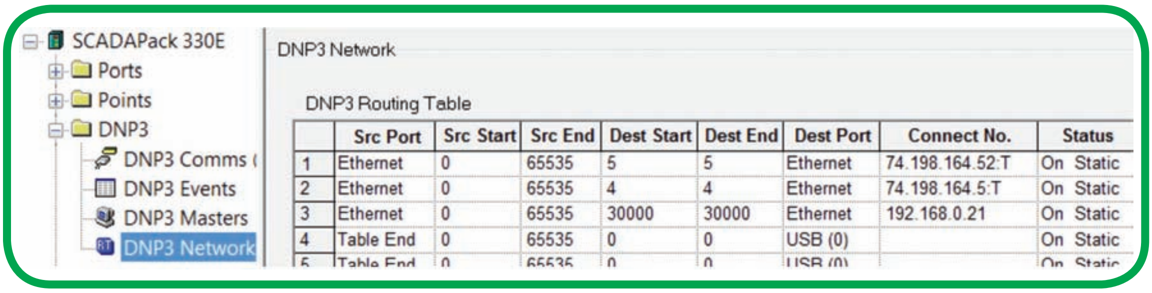
Let's say that in our example network, as shown in Figure 5, ClearSCADA as the master station (host) has IP address 192.168.1.100 and our Gateway RTU has address 192.168.1.101. Thus ClearSCADA will send all of its messages for remote RTUs to IP address 192.168.1.101, even though each remote RTU's DNP3 address will be unique. When the message is routed by the Gateway RTU, it traverses the firewall and IP router and goes out onto the telecommunication network via the Backhaul link.

The 192.168.1.101 address of the SCADAPack E Gateway RTU is not used beyond the IP router; instead the message needs to have the fixed IP address of the router on the Backhaul link side. This Backhaul link IP address will be the address that the remote RTUs will receive messages from, and so respond to. This is important because the remote RTUs will actually appear to be communicating with the router's fixed IP address on TCP port 20000. However, the IP router's job is to accept messages on TCP port 20000 and then route them to the appropriate internal IP address, in this example to 192.168.1.101. This is known as Network Address Translation (NAT). Your network administrator can set this up.

Gateway RTU Configuration

Figure 6 shows the DNP3 Routing Table configuration for the Gateway RTU. In summary, row 1 causes all DNP3 messages received at the Gateway RTU for RTU 5 to be routed to its appropriate IP address via Ethernet. Row 2 routes received messages for the host (address 30000) to the host's IP address. In the example described above, row 2's "Connect No." field would be configured as the master station (host) IP address of 192.168.1.100.

Please see **Appendix A** for definitions of the routing table fields.



DNP3 Network

DNP3 Routing Table

	Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect No.	Status
1	Ethernet	0	65535	5	5	Ethernet	74.198.164.52:T	On Static
2	Ethernet	0	65535	4	4	Ethernet	74.198.164.5:T	On Static
3	Ethernet	0	65535	30000	30000	Ethernet	192.168.0.21	On Static
4	Table End	0	65535	0	0	USB (0)		On Static
5	Table End	0	65535	0	0	USB (0)		On Static

• Figure 6: Gateway RTU DNP3 routing table configuration

By way of a more detailed explanation of the routing table contents, the configuration shown in Figure 6 is explained: the first row in the routing table indicates that messages coming from (the *source*) Ethernet Port with DNP3 addresses between 0 and 65535 (i.e. any DNP3 address), and going to (the *destination*) DNP3 address 5 are to be routed out of the Ethernet port (Dest Port) to IP address 74.198.164.98 using TCP transport (as shown in the *Connect No.* string). The *Dest Start* & *Dest End* entries are both the same and so refer to just one DNP3 device address rather than a range of addresses. The Status column is set to *On Static*, which is significant in this case. *On Static* means, as described in Appendix A, that this route was created by the user, but will be updated automatically. This allows the Gateway RTU to detect traffic from RTU 5, and if it is found to have a different IP address, it will change the IP address in this table so that all future messages routed to RTU 5 are sent to the new IP address.

The third row in Figure 6 is a route to the host (master station, whose DNP3 device address is 30000) at IP address 172.20.5.101. All traffic bound for the host, in this example a ClearSCADA server, will be routed to IP address 172.20.5.101 using TCP. With a single host server, the *Status* could be set to *On Fixed* (meaning that this routing entry will always stay the same and will not update automatically). However, if host server redundancy is to be used, the *Status* should be set to *On Static* so that a change in host server IP address can be updated automatically.

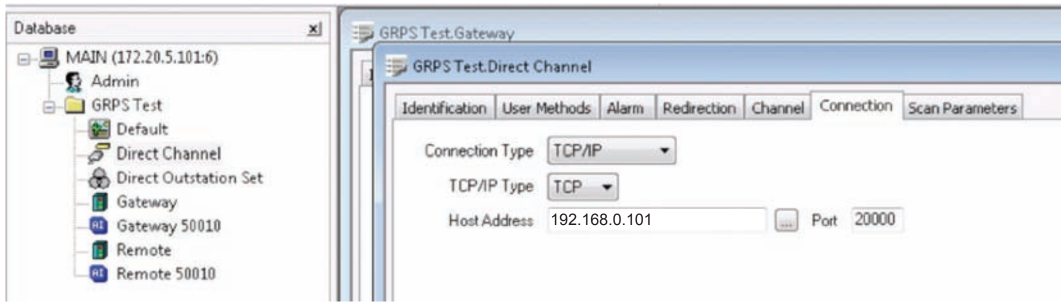
Master Configuration

Adapt these example configurations if you are using a different Master device.

In the host configuration it is important to understand the required configuration parameters. Since we must rely on the Gateway RTU to route all DNP3 messages, it stands to reason that all DNP3 messages from the host, regardless of which remote RTU, must be directed to the Gateway RTU first. It will then route the message to the remote RTU appropriately. In ClearSCADA, this can be done by setting up a Channel object as shown in Figure 7.

On the Connection tab, the Connection Type is set to TCP/IP which allows the user to enter an IP address. This type of configuration allows ClearSCADA to communicate with all devices attached to that channel by sending the messages to this specific address. In this case, the IP configured should be the IP address of the Gateway RTU.

On the Outstation object, as shown in Figure 8, the only configuration parameter which differs from a standard configuration when using Serial or direct IP connections is on the Network tab, where in this case the “Network” type should be set to “None”. (A result of specifying the TCP/IP Connection Type as shown in Figure 7).

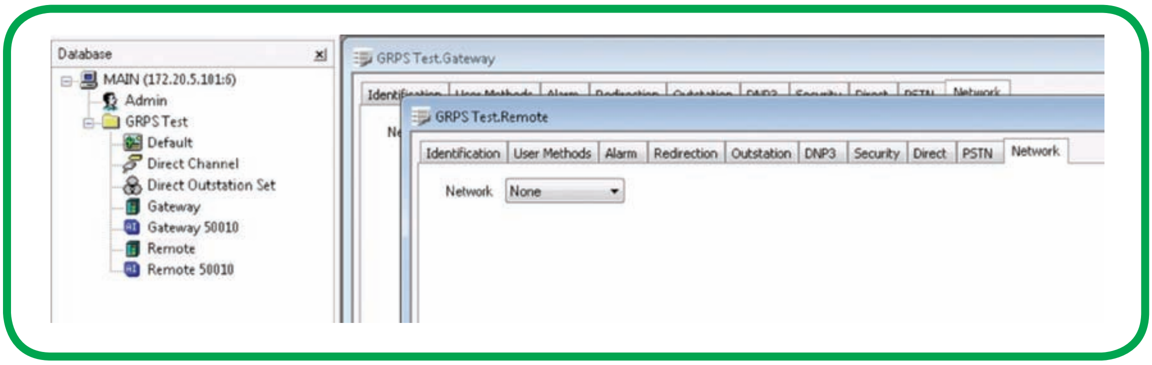


Connection Type TCP/IP

TCP/IP Type TCP

Host Address 192.168.0.101 Port 20000

• Figure 7: SCADA sever DNP3 channel configuration



Network: None

- Figure 8: SCADA server DNP3 device configuration

Remote RTU Configuration

Note: *the following information is intended to show the additional settings required for the remote RTU in this scenario. Note this is not a guide on how to setup a SCADAPack E RTU.*

Figure 9 shows the typical configuration settings for the SCADAPack E RTU for a GPRS modem. On the GPRS page, the Port Function (for Port 1 in this case) should be set for *PPP/TCPIP*. The *Port Mode* should be set to GPRS.

The *Port Init. String* should be updated if the modem has particular requirements. For example when using the Schneider Electric SR2MOD03 modem in the Americas use:

ATE0V0&D2+WIND=0;+WOPEN=0;+CREG=0; +CGREG=0;+WMBS=4

For the SR2MOD03 in the rest of the world use:

ATE0V0&D2+WIND=0;+WOPEN=0;+CREG=0; +CGREG=0;+WMBS=5

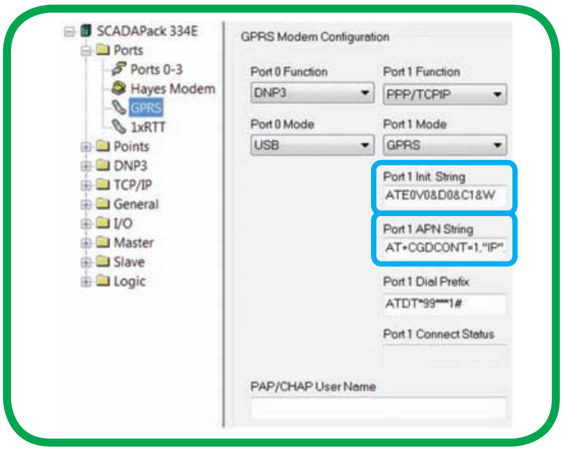
For more information on using the Schneider Electric SR2MOD03 GPRS modem with the SCADAPack E refer to the Schneider Electric technical note “Using SR2MOD03 Modems for Telemetry and Remote SCADA”.

The APN name for the telecommunications service provider should also be updated as shown in Figure 9, substituting the APN name in double quotes at the end of the *Port APN String* field. For example:

AT+CGDCONT=1,”IP”,”INTERNET.COM”

If provided by the telecommunications service provider, enter the service User Name and Password.

The RTU’s DNP3 Master configuration is set to the DNP3 device address of ClearSCADA, in this case 30000 (see Figure 10).



GPRS Modem Configuration

Port 0 Function: DNP3

Port 1 Function: PPP/TCPIP

Port 0 Mode: USB

Port 1 Mode: GPRS

Port 1 Init. String: ATE0V0&D0&C1&W

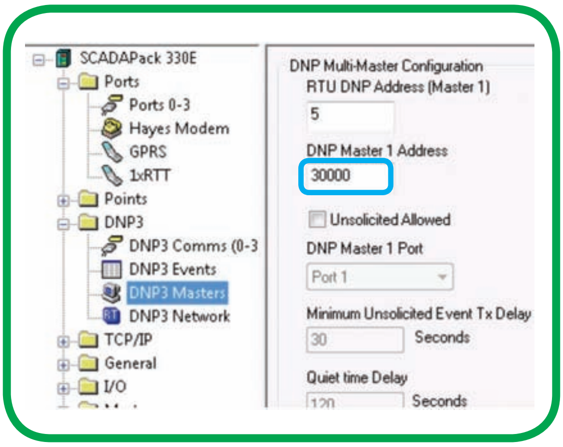
Port 1 APN String: AT+CGDCONT=1,"IP",

Port 1 Dial Prefix: ATDT*99***1#

Port 1 Connect Status:

PAP/CHAP User Name:

- Figure 9: Remote RTU configuration for GPRS



DNP Multi-Master Configuration

RTU DNP Address (Master 1): 5

DNP Master 1 Address: 30000

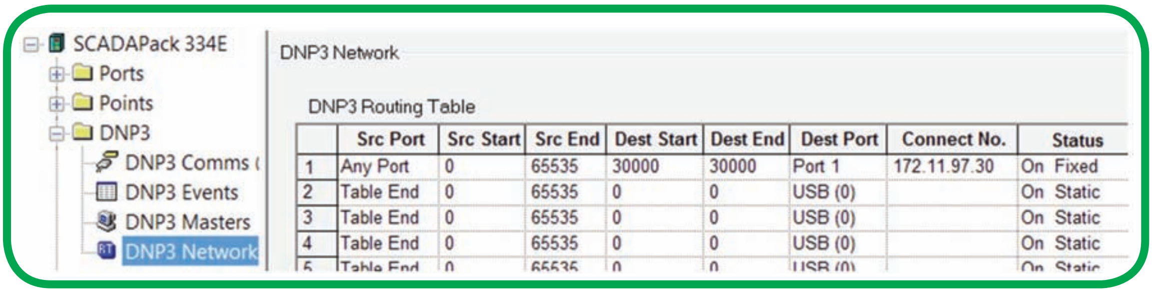
□ Unsolicited Allowed

DNP Master 1 Port: Port 1

Minimum Unsolicited Event Tx Delay: 30 Seconds

Quiet time Delay: 120 Seconds

- Figure 10: Remote RTU configuration for DNP3 master station communication



DNP3 Network

DNP3 Routing Table

	Src Port	Src Start	Src End	Dest Start	Dest End	Dest Port	Connect No.	Status
1	Any Port	0	65535	30000	30000	Port 1	172.11.97.30	On Fixed
2	Table End	0	65535	0	0	USB (0)		On Static
3	Table End	0	65535	0	0	USB (0)		On Static
4	Table End	0	65535	0	0	USB (0)		On Static
5	Table End	0	65535	0	0	USB (0)		On Static

• Figure 11: Remote RTU routing table configuration

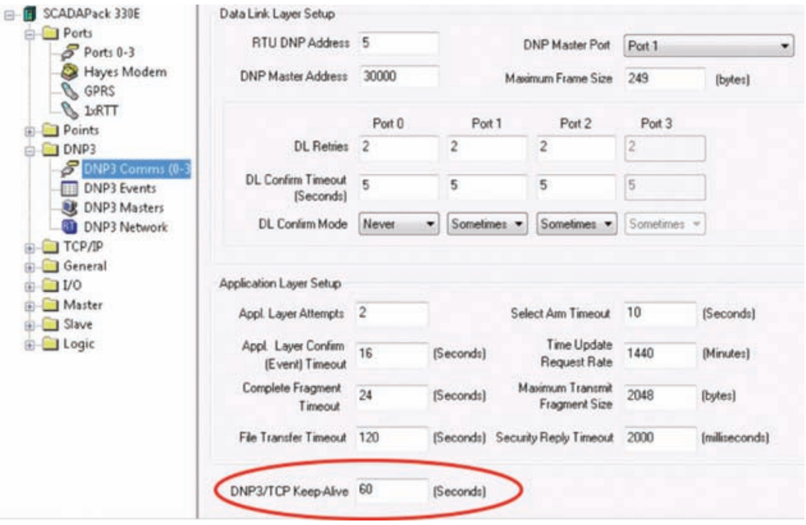
The routing table in the remote RTU is configured to send all data to the Gateway RTU as shown in Figure 11. This should be the fixed IP address of the IP router on the Backhaul link side.

The remote RTU's routing table is instructing the RTU to send IP messages out on Port 1 which is a serial port.

This is due to the fact that in this example the RTU is using PPP communications with a GPRS modem connected to RTU Port 1 (PPP is a serial protocol for IP communication).

With this configuration, all data from the remote RTU will be sent via the Gateway RTU, which will then be responsible for routing the data on to the host (master station).

Appendix A describes the routing table fields.



Data Link Layer Setup

RTU DNP Address 5

DNP Master Port Port 1

DNP Master Address 30000

Maximum Frame Size 249 (bytes)

	Port 0	Port 1	Port 2	Port 3
DL Retries	2	2	2	2
DL Confirm Timeout (Seconds)	5	5	5	5
DL Confirm Mode	Never	Sometimes	Sometimes	Sometimes

Application Layer Setup

Appl. Layer Attempts 2

Select Arm Timeout 10 (Seconds)

Appl. Layer Confirm (Event) Timeout 16 (Seconds)

Time Update Request Rate 1440 (Minutes)

Complete Fragment Timeout 24 (Seconds)

Maximum Transmit Fragment Size 2048 (bytes)

File Transfer Timeout 120 (Seconds)

Security Reply Timeout 2000 (milliseconds)

DNP3/TCP Keep-Alive 60 (Seconds)

• Figure 12: Remote RTU DNP3/TCP Keep-Alive timer configuration

Lastly, the DNP3/TCP Keep-Alive setting is configured in the remote RTU (see Figure 12). This is very important as it is the main way of ensuring that the remote site RTU remains connected to the Gateway RTU and available for the master station to communicate with it.

In a dynamic IP based GPRS network it is usual for the network to silently disconnect a device after a period of inactivity. It is the devices responsibility to maintain the connection. The simplest way to do this is using the DNP3/TCP Keep-Alive that periodically sends a small DNP3 data link message.

The value of this parameter is an important consideration. DNP3/TCP Keep-Alive messages must be sent more often than the network disconnection time, not so often as to be a significant communication overhead, but often enough to minimize the reconnection interval if an unexpected communication interruption occurs. In general it should be set slightly longer than the poll interval, but slightly less than the network disconnection time.

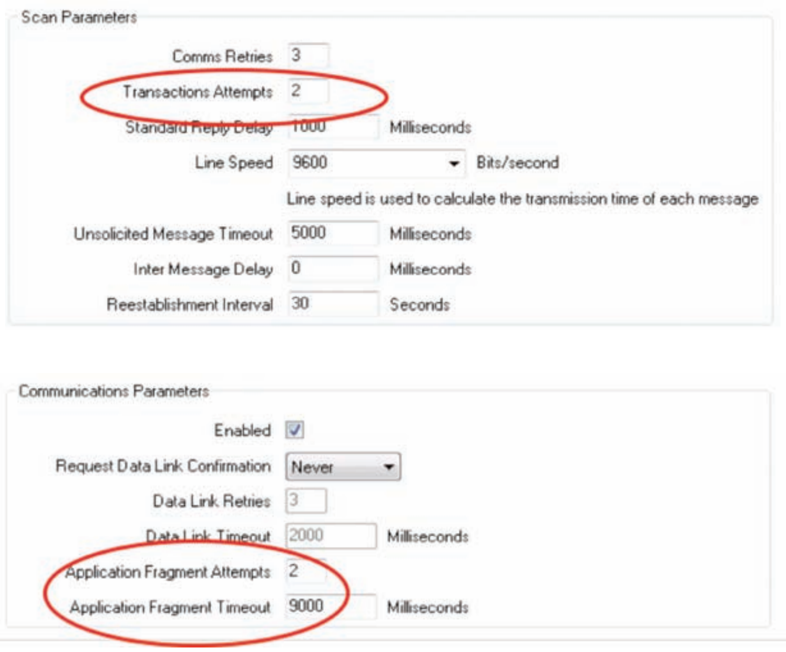
By setting the DNP/TCP Keep-alive time lower than a poll rate, the keep-alive messages will be suppressed while the polling is successful.

The following examples assume a network disconnection time of *20 minutes*.

Master Station Polling Rate	Example remote RTU DNP/TCP Keep-alive time
60 secs	60 secs
5 minutes	5 minutes
30 minutes	30 minutes
2 hours	2 hours

If the GPRS network assigns a new IP address to the remote RTU, the RTU will send an additional DNP/TCP keep-alive message, updating the Gateway RTU with the remote RTU's new IP address, before the message is routed to the master station.

Suggested master station communication settings to provide some tolerance to GPRS network characteristics are shown in Figure 13.



Scan Parameters

Comms Retries 3

Transactions Attempts 2

Standard Reply Delay 1000 Milliseconds

Line Speed 9600 Bits/second

Line speed is used to calculate the transmission time of each message

Unsolicited Message Timeout 5000 Milliseconds

Inter Message Delay 0 Milliseconds

Reestablishment Interval 30 Seconds

Communications Parameters

Enabled ☑

Request Data Link Confirmation Never

Data Link Retries 3

Data Link Timeout 2000 Milliseconds

Application Fragment Attempts 2

Application Fragment Timeout 9000 Milliseconds

• Figure 13: SCADA server DNP3 configuration parameters

Advanced Topics

Security Considerations

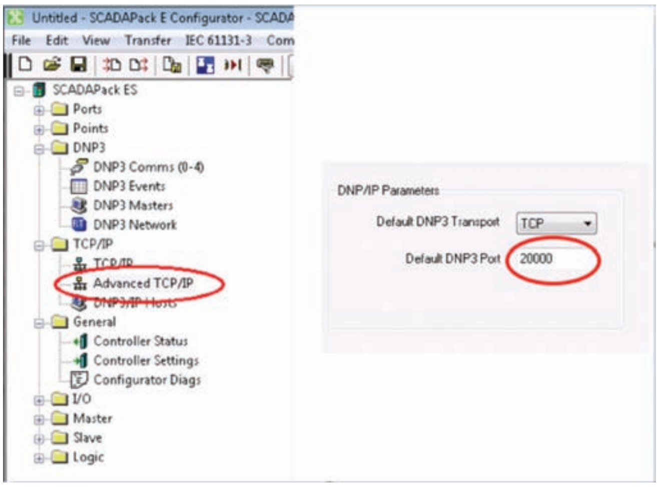
It is best to avoid using an open public IP network service if possible. Consider one or more of the following:

- Talk with your telecommunication services provider about a private APN solution to restrict public access to your cellular devices, or about providing a VPN solution between the cellular modems and the router, where possible
- Use SCADAPack E DNP3 Secure Authentication. This is fully supported using the same architecture as shown, provided that the master station (host) supports DNP3 Secure Authentication
- Use SCADAPack E AGA12 encryption solution for DNP3 between the Gateway RTU and the remote RTUs (there are no special requirements for the Remote SCADA Master, however this option may not be available in your location due to export restrictions)
- Use a firewall between the SCADAPack E Gateway RTU and the telecommunication network
- Disable IP services such as Telnet, FTP, NTP, Modbus/TCP on all remote RTUs when the services are not in use

System Expansion

If there is a need to expand the system past the maximum recommended numbers of remote RTUs connected per gateway (25 for a Gateway RTU using a SCADAPack 300E; 90 for a Gateway RTU using a SCADAPack ES) there will need to be extra Gateway RTU devices added. To achieve this, the following will need to be implemented:

- Set the additional Gateway RTU's Advanced TCP / *Default DNP3 Port* number (see Figure 14) to a different port number than any other Gateway RTU on the network. (This is referring to the IP port number for DNP3 which is by default 20000. Change it to something different, e.g. 20001). IP router configurations are simpler if they translate one port number per fixed IP address, so subsequent Gateway RTUs will each need to use different ports for the DNP3 communications
- Set the same default port number on each remote RTU that will communicate via the new gateway RTU
- Add another entry in the network IP router, using the new port number, for the new gateway RTU
- Add another channel configuration in the master station using the new gateway RTU's IP address and port number (e.g. 20001)



DNP/IP Parameters

Default DNP3 Transport: TCP

Default DNP3 Port: 20000

• Figure 14: Changing the Default DNP3 port number

Other Topics of Interest

This architecture is not limited to being used simply for master to remote RTU communications. This architecture will also support:

- Remote management of SCADAPack E RTUs using the SCADAPack E Configurator.

  When connecting to a remote RTU from the same LAN as the master station (host), use the IP address of the Gateway RTU in the Configurator. Use either TCP or UDP communication. A USB connection directly to the Gateway RTU could also be used. Set the Target DNP3 Address in the Configurator to be the address of the remote RTU. The Gateway RTU will route messages to the remote RTU for the Configurator in the same way that it does for the master station (host).

  A connection of a Configurator from a remote RTU from another remote RTU is also possible. See the next description on setting up Peer-to-Peer communication.

  Note that in a dynamic IP network such as GPRS, the TCP connection necessary for communication is initiated from the cellular device. Connections cannot be made to remote RTUs where they are initiated from the master station (host) network. This includes FTP, Telnet, etc.

- Peer-to-Peer communications, whereby two or more remote RTU devices can talk with each other. To achieve this, routing table entries in the remote RTUs must include the other peer RTU(s) it will communicate with. Keep in mind that all the traffic will be routed through the Gateway RTU. So the new routing table entries for the peer RTUs would specify the DNP3 address of the peer remote RTU but would specify the fixed IP address of the IP router's backhaul link in order to contact the Gateway RTU

- Redundant SCADA masters (such as in the case of a main / standby server pair for ClearSCADA). In this case ensure that the routing table entry in the Gateway RTU (for the host) is configured as *On Static* rather than *On Fixed*. With *On Static*, if the master changes to a server with a different IP address, the DNP routing table will automatically be updated with the IP of the new master; communication continues to function without any user input

Appendix A

Source for this information is located in the SCADAPack E online Reference Manuals at:

SCADAPack E Configurator User Manual > Configurator Property Pages > DNP3 Folder > ***DNP3 Network Property Page***

The **DNP Node Routing Table** is a grid layout with each row containing one routing table entry. Each entry describes one scenario for routing of DNP3 frames received at this node. When searching for a route entry, the routing table is scanned from top to bottom for a matching entry. Scanning stops at the first matching entry, or at the first Table **End** entry in the **Src Port** field.

Source Port

The **Src Port** field refers to the port on which the inbound DNP3 frame arrived at the E-Series RTU. The DNP3 driver matches the Source Port (**Src Port**), and the Source Start (**Src Start**)/ Source End (**Src End**) range as part of the route filtering. The Src Port may be selected as any **serial port**, **Ethernet port**, **Any Port**, or Table **End**.

Source Start and Source End

The **Src Start** and **Src End** fields specify the range of source DNP3 addresses to which this routing table entry refers. The normal range is 0 – 65535, which matches any DNP3 frame originating from any DNP3 node.

Destination Start and Destination End

The **Dest Start** and **Dest End** fields specify the range of destination DNP3 addresses to which this routing table entry refers.A packet received by this RTU going to an RTU in this range will be routed to the **Dest Port** (providing the source filtering is satisfied).

Destination Port

The **Dest Port** field specifies which RTU Port the DNP3 frame will be re-transmitted (forwarded) on.

Connect Number

The **Connect No.** field specifies the connection number (e.g., Phone number, X.25 address, or IP address) to reach the destination DNP3 node(s). The routing table is used to store connection numbers of RTUs or other devices that will be directly dialed. Therefore, a routing table entry needs to exist for each remote device with which the RTU intends to communicate using a PSTN, GSM, or TCP/IP host.

When routing using DNP3 over IP networks, valid IP Address Formats for “Connect No.” field are:

nnn.nnn.nnn.nnn	IP address only e.g. 192.168.0.249
*nnn.nnn.nnn.nnn:*T	use TCP transport e.g. 192.168.0.249:T
*nnn.nnn.nnn.nnn:*U	use UDP transport e.g. 192.168.0.249:U
*nnn.nnn.nnn.nnn:*pppppU	use UDP port number e.g. 192.168.0.249:7001U

When routing using dial-up networks, the **Connect No.** field should contain the telephone number of the remote device.

Status

The **Status** field indicates the status of this routing table entry and may be one of the following values:

- **On Static** - User entered route
- **Off Static** - User entered route (Disabled)
- **On Dynamic** - Automatically generated route (e.g. for Configurator communication with the RTU)
- **Off Dynamic** - Automatically generated route with an expired lifetime
- **On Fixed** - User entered route: will NOT be updated by communication activity
- **Off Fixed** - User entered route (Disabled)

Schneider Electric

Telemetry & Remote SCADA Solutions
48 Steacie Drive, Kanata, Ontario K2K 2A9 Canada
Direct Worldwide: 1 (613) 591-1943
Fax: 1 (613) 591-1022
Toll Free within North America: 1 (888) 267-2232
www.schneider-electric.com