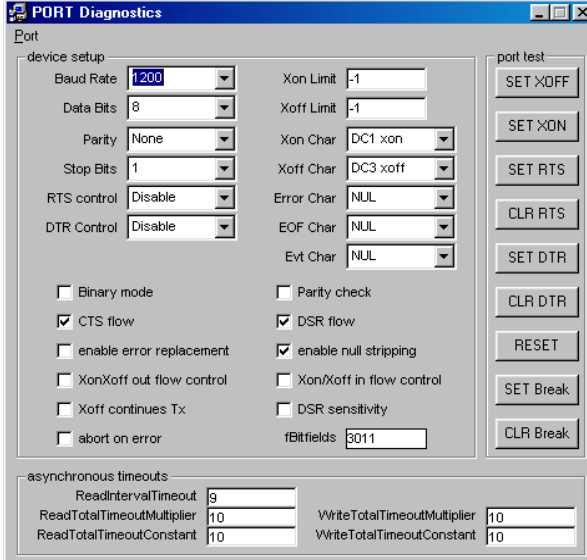


MODBUS Diagnostic aid

This diagnostic aid tests MODBUS protocol installations, by simulating either a MODBUS master or slave device in RTU or ASCII mode. Functions 1 (read coils), 2 (read coils), 3 (read input registers) ,4 (read holding registers), 5 (force single coil), 6 (precept single register) and 16 (diagnostics) are implemented. Functions 1 and 2 are considered identical in operation, as are functions 3 and 4. When operating in MASTER mode, the request to read registers is limited to enquire on 16 consecutive registers. The MASTER is also configured to enquire on 16 coils, sufficient to pack into a 16-bit word.

When the application is first invoked, it will be necessary to: -

- Select the COM port over which the MODBUS device will communicate. All available devices are added to the menu and it is necessary to simply select the device from the menu.
- It is likely that the selected port will also need configuring before it will work; in particular check whether or not RTS and CTR control are required. Incorrect setting of these will prevent apparent communication.
- Set the computer number to something other than zero. Zero in MODBUS protocol signifies a broadcast address.
- Decide whether to operate in MASTER or SLAVE mode; MASTER will initiate enquiries, whilst SLAVE will respond.
- The port test buttons on the right of the display can be used in conjunction with a breakout box to check on port status.



The screenshot shows the 'PORT Diagnostics' window. It is divided into several sections:

- device setup:** Includes dropdown menus for Baud Rate (1200), Data Bits (8), Parity (None), Stop Bits (1), RTS control (Disable), and DTR Control (Disable). It also has input fields for Xon Limit (-1), Xoff Limit (-1), Xon Char (DC1 xon), Xoff Char (DC3 xoff), Error Char (NUL), EOF Char (NUL), and Evt Char (NUL).
- port test:** A vertical column of buttons on the right side, including SET XOFF, SET XON, SET RTS, CLR RTS, SET DTR, CLR DTR, RESET, SET Break, and CLR Break.
- checkboxes:** A group of checkboxes for Binary mode, CTS flow (checked), enable error replacement, Xon/Xoff out flow control, Xoff continues Tx, abort on error, Parity check, DSR flow (checked), enable null stripping, Xon/Xoff in flow control, and DSR sensitivity.
- asynchronous timeouts:** Input fields for ReadIntervalTimeout (9), ReadTotalTimeoutMultiplier (10), ReadTotalTimeoutConstant (10), WriteTotalTimeoutMultiplier (10), and WriteTotalTimeoutConstant (10).
- fBitfields:** An input field containing the value 3011.

Figure 1 - PORT Set-up

MODBUS Diagnostic aid

SLAVE MODE

Operation in slave mode gives the opportunity to configure up to 128 registers (0 to 127 inclusive) with different values and functions, and up to 128 coils (0 to 127).

- First use the drop-down box to select the register to configure.
- Set the Min and Max values that the register should contain.
- Set the interval over which this range should operate. A sensible choice would be 1 hour, but other values can be set.
- Select the function to use. Ramp will take the register from the minimum value to the maximum value over the selected time interval, the direction being determined by selection. The step function will hold a register at a set Min value for the time interval then at the Max value for the same time interval. The cyclic function will generate a complete sinusoid ranging between Min and Max over the selected time interval. Static will not change the register value at all.
- Once the registers are all configured, you may wish to save the register settings in the menu pull-down.
- The START button will start a timer used to control the current values of the registers.
- The Display Request option will allow the requests from the MASTER and the responses to be observed on the screen.

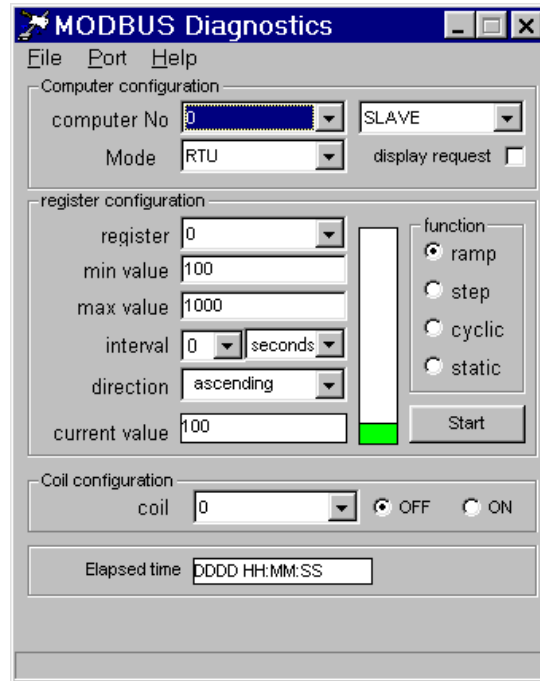


Figure 2 - SLAVE MODE

Since the SLAVE diagnostic can only configure 128 registers and the address space is a 16-bit number, bits 11 to 15 of the starting address are used to hold flags to determine what is to be returned from the SLAVE. This is useful if 32-bit values are to be returned for example.

- Registers in the range 0-127 (0000-007F) are 16-bit registers.
- Registers in the range 128-255 (0080-00FF) have an implied 1 DP (i.e. scaled by a factor of 10). (Bit 11 of starting address = 1)
- Registers in the range 256-383 (0100-017F) are long integers with the most significant word first. (Bit 12 of starting address = 1)
- Registers in the range 384-511 (0180-01FF) are long integers with the least significant word first. (Bit 13 of starting address = 1)
- Registers in the range 512-639 (0200-027F) are long integers with the least significant word first. (Bit 13 of starting address = 1)
- Registers in the range 640-767 (0280-02FF) are long integers with the most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 768-895 (0300-037F) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 896-1023 (0380-03FF) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1024-1151 (0400-047F) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1152-1279 (0480-04FF) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1280-1407 (0500-057F) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1408-1535 (0580-05FF) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1536-1663 (0600-067F) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1664-1791 (0680-06FF) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1792-1919 (0700-077F) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 1920-2047 (0780-07FF) are floating point numbers, treated as long integers, most significant word first. (Bit 14 of starting address = 1)
- Registers in the range 2048-2175 (0800-087F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2176-2303 (0880-08FF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2304-2431 (0900-097F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2432-2559 (0980-09FF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2560-2687 (0A00-0A7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2688-2815 (0A80-0AFF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2816-2943 (0B00-0B7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 2944-3071 (0B80-0BFF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3072-3199 (0C00-0C7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3200-3327 (0C80-0CFF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3328-3455 (0D00-0D7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3456-3583 (0D80-0DFF) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3584-3711 (0E00-0E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3712-3839 (0E80-0E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3840-3967 (0F00-0F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 3968-4095 (0F80-0F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4096-4223 (1000-107F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4224-4351 (1080-107F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4352-4479 (1100-117F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4480-4607 (1180-117F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4608-4735 (1200-127F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4736-4863 (1280-127F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4864-4991 (1300-137F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 4992-5119 (1380-137F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5120-5247 (1400-147F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5248-5375 (1480-147F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5376-5503 (1500-157F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5504-5631 (1580-157F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5632-5759 (1600-167F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5760-5887 (1680-167F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 5888-6015 (1700-177F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6016-6143 (1780-177F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6144-6271 (1800-187F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6272-6399 (1880-187F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6400-6527 (1900-197F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6528-6655 (1980-197F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6656-6783 (1A00-1A7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6784-6911 (1A80-1A7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 6912-7039 (1B00-1B7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7040-7167 (1B80-1B7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7168-7295 (1C00-1C7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7296-7423 (1C80-1C7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7424-7551 (1D00-1D7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7552-7679 (1D80-1D7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7680-7807 (1E00-1E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7808-7935 (1E80-1E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 7936-8063 (1F00-1F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8064-8191 (1F80-1F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8192-8319 (2000-207F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8320-8447 (2080-207F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8448-8575 (2100-217F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8576-8703 (2180-217F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8704-8831 (2200-227F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8832-8959 (2280-227F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 8960-9087 (2300-237F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9088-9215 (2380-237F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9216-9343 (2400-247F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9344-9471 (2480-247F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9472-9599 (2500-257F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9600-9727 (2580-257F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9728-9855 (2600-267F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9856-9983 (2680-267F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 9984-10111 (2700-277F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10112-10239 (2780-277F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10240-10367 (2800-287F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10368-10495 (2880-287F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10496-10623 (2900-297F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10624-10751 (2980-297F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10752-10879 (2A00-2A7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 10880-11007 (2A80-2A7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11008-11135 (2B00-2B7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11136-11263 (2B80-2B7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11264-11391 (2C00-2C7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11392-11519 (2C80-2C7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11520-11647 (2D00-2D7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11648-11775 (2D80-2D7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11776-11903 (2E00-2E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 11904-12031 (2E80-2E7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12032-12159 (2F00-2F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12160-12287 (2F80-2F7F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12288-12415 (3000-307F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12416-12543 (3080-307F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12544-12671 (3100-317F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)
- Registers in the range 12672-12799 (3180-317F) are floating point numbers, treated as long integers, least significant word first. (Bit 15 of starting address = 1)

In deciding which values to return, the SLAVE will examine the 5 most significant bits of the starting address and treat them as flags. The flags are mutually exclusive with the most significant bit taking priority over the least.

MODBUS Diagnostic aid

The SLAVE simulator is also configured to respond to diagnostics messages. The diagnostics functions can only handle 16-bit register addresses and 16-bit data responses because of the MODBUS packet structure.

The following sub-functions have been implemented.

- 0 =loopback message
- 1 =restart (zeros all counters and timers, resets to defaults, exit listen mode)
- 2 =return the diagnostic register contents
- 3=change ASCII delimiter (which has a default of LF)
- 4 =change to listen mode
- 10 =clear counters (a sub-set of restart)
- 11 =return bus message count
- 12 =return CRC communication error count
- 13 =return exception error count
- 14 =return slave message count
- 15 =return slave no response count
- 16 =return slave NAK count
- 17 =return slave busy count
- 18 =return port data overrun error count

The SLAVE device will respond with appropriate messages for any unrecognised functions or any registers out of range or invalid data values. Any error counts or register values will be returned as a 16-bit value.

MODBUS Diagnostic aid

MASTER MODE

Operation in MASTER mode will display extra options.

All registers are normally in the range 30000 to 40000 in keeping with MODBUS protocol, but since the enquiry only makes a relative request, the relative register addresses are those given above.

Initial set-up is similar to that for the SLAVE mode. Select the communication port, configure the port. Operating the single-shot button will make a single request to the SLAVE device. If the register requested is the one displayed its value will be displayed in the current value box. Clicking the single shot will actually make two enquiries of the SLAVE; first for 16 coils (and process the response), then for 32 registers. If the registers are long registers this will actually make an enquiry for the correct number of 16-bit values and process the response accordingly.

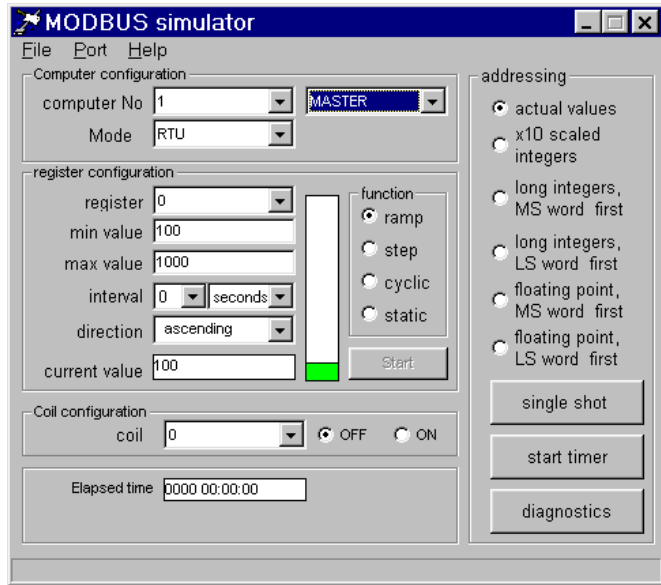


Figure 3 - MASTER MODE

The diagnostics button will give access to another window which will make single requests to the SLAVE for a selected value. It can also be used to preset a single register or force a single coil. Dependent upon which function is selected, appropriate drop-down boxes and text entry boxes will be enabled for completion of the request. Requests and responses will always be visible in the window (in ASCII or HEX format). Error returns, where recognised will be interpreted in the status box at the bottom of the window.

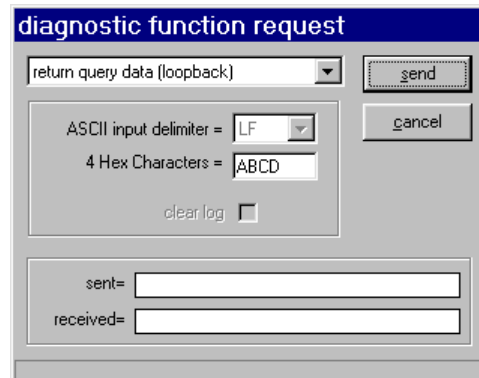


Figure 4 - Diagnostics functions

As a test, two copies of this utility can be operated on the same PC through two separate COM ports cabled together with a null-modem (x-over) cable, with one of the applications configured as MASTER and the other as SLAVE.

MODBUS Diagnostic aid

REPORTS.

Reports can be set up and scheduled using this screen. Tick the boxes for the required items to be included in the report. The report format is a CSV file which can be read by other applications such as Excel. The name of the report can be a single filename, in which case a new report will over-write any existing report of the same name. A unique filename will append a date and timestamp to the filename to make it unique and they will all be deposited in the same directory.

The screenshot shows a 'schedule reports' dialog box with the following configuration:

- Frequency: Never, Once, Hourly, Daily, Weekly
- Schedule: on a at :
- Filename: unique filename, single filename
- filespec: ...
- include in report...:
 - register or coil no
 - description
 - min value
 - max value
 - date & time stamp
 - current value

Figure 5 - scheduling reports