

ACCES I/O eNET Advanced Features

This document describes the advanced configuration features of the ACCES I/O eNET. It covers:

1. ACCES I/O eNET port modes
2. Virtual port (driver) settings
3. Virtual port (driver) bindings
4. Virtual port COM number assignment
5. Transmit FIFO buffer configuration
6. WAN Port configuration

1. ACCES I/O eNET port modes

The ACCES I/O eNET converts serial port data to and from TCP/IP packets over Ethernet. Each ACCES I/O eNET port exchanges TCP/IP packets on its own unique TCP port (called the "Local Port" in the Properties dialog box). Each serial port on an ACCES I/O eNET device can be configured independently to perform this conversion in one of eight modes:

Driver Mode (Default mode)

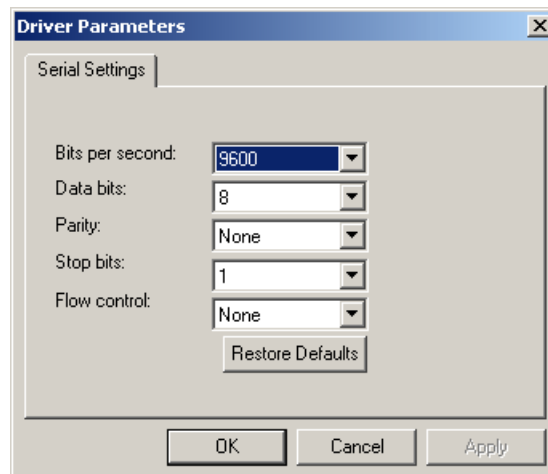
This mode enables the physical port of an ACCES I/O eNET to communicate directly with the serial port API of a supported operating system as a local COM port. In this mode, authorized users can set bits per second, data bits, parity, stop bits, and flow control port-by-port, or the port will accept its serial port settings from the application/operating system that is accessing it. Driver mode is the factory default mode when an ACCES I/O eNET is installed.

When installed on a LAN, an ACCES I/O eNET in Driver Mode has all the functionality of an internally installed serial port.

When installed on a WAN or the Internet, the serial port of an ACCES I/O eNET gains enormous flexibility and power. To use an ACCES I/O eNET port on a remote network:

1. configure the IP address and TCP port of the WAN connection in the *eNET-Manager* to match the gateway IP address of the remote network,
2. map the IP address and TCP port of the remote gateway to the IP address of the ACCES I/O eNET, and
3. configure the ACCES I/O eNET itself for Driver Mode.

Applications: General serial port access from applications running on a PC.

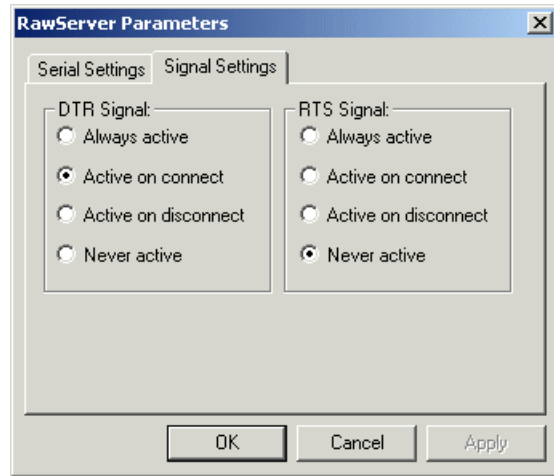
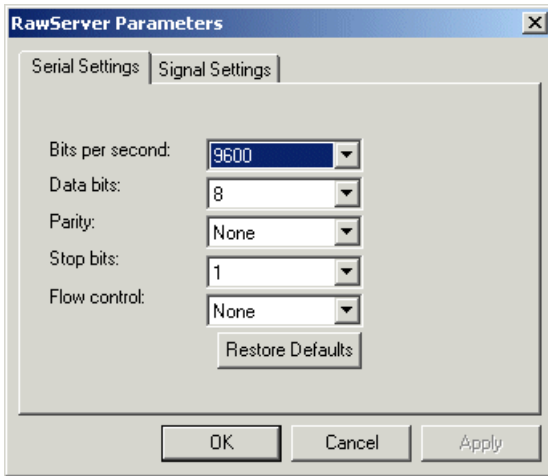


Raw Server Mode

This mode is used to establish a raw TCP connection to an ACCES I/O eNET port. The physical port on the ACCES I/O eNET is made available as a network resource with a specified IP address and port number. In this mode, authorized users can set bits per second, data bits, parity, stop bits, and flow control port-by-port, to match the requirements of the Data Terminal Equipment (DTE) connected to the physical ACCES I/O eNET port.

Control lines can be triggered by the TCP connection being established. Under the "Signal Settings" tab shown below, the user can set how the control lines are to react when a TCP connection is established.

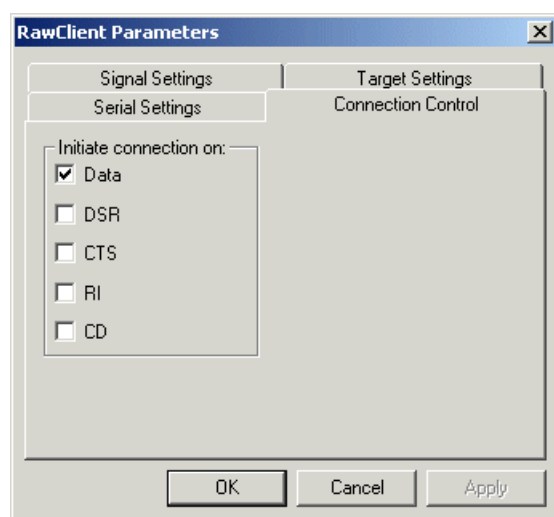
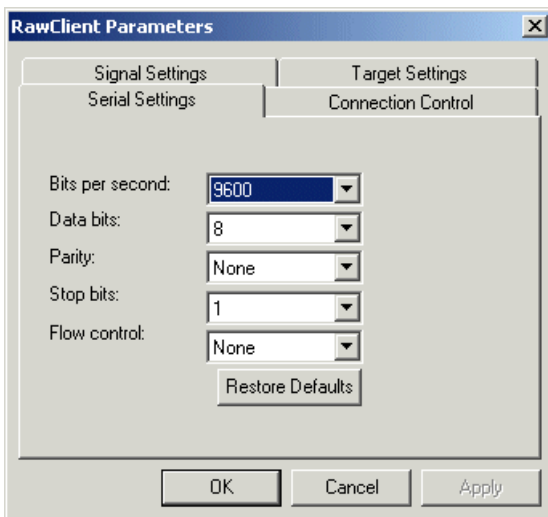
Applications: Remote monitoring, security systems.

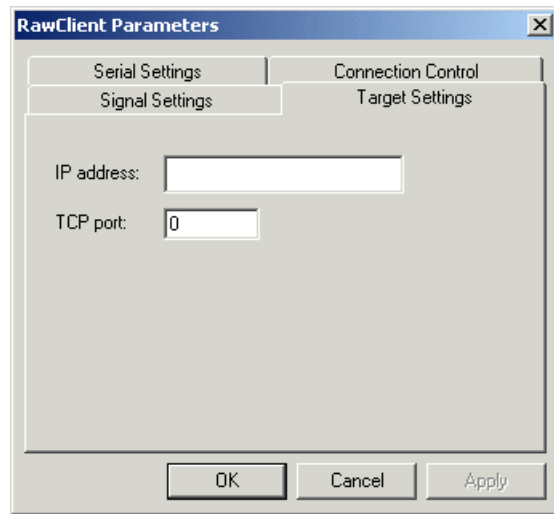
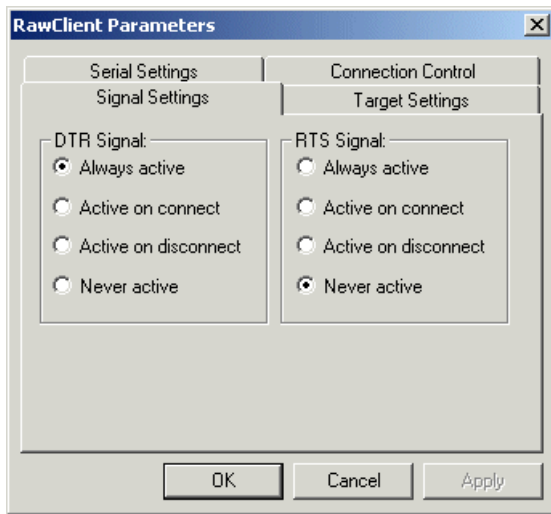


Raw Client Mode

This mode is used to establish a raw connection to the ACCES I/O eNET. The physical port on the ACCES I/O eNET is configured to initiate a connection to a pre-defined IP address and port number, specified by an authorized user of that port in the "Target Settings" dialog box. In this mode, authorized users set bits per second, data bits, parity, stop bits, and flow control port-by-port, to match the requirements of the Data Terminal Equipment (DTE) connected to the physical ACCES I/O eNET port. Operating as a client, the ACCES I/O eNET will open a connection to the target IP address and port when it detects one or more of the following line conditions: data, DSR, CTS, RI, or CD. Users can configure which of these triggers will be in effect for any ACCES I/O eNET port set in this mode in the "Connection Control" dialog box. "Signal Settings" are also settable by the user, as described in Raw Server mode.

Application: Remote control.



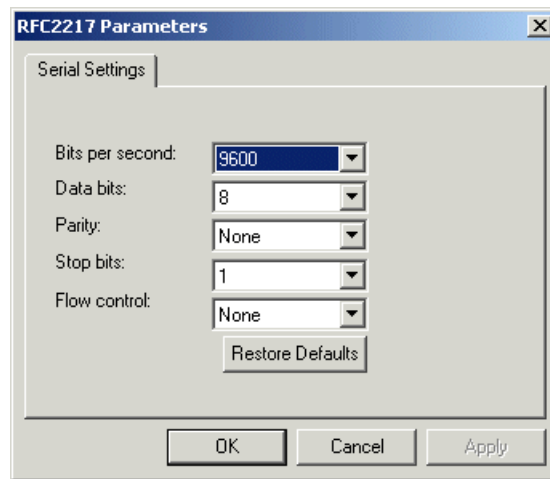


RFC2217 Mode

Users who want to communicate with an ACCES I/O eNET across gateways or routers can configure a port on an ACCES I/O eNET to operate in RFC 2217 mode, allowing serial port configuration commands and serial data to be sent to an ACCES I/O eNET using the RFC 2217 framework for serial port control over Telnet. For those not familiar with RFC 2217 (the Telnet COM Port Control Option), the text of the actual RFC (Request For Comments) is available at www.faqs.org/rfcs/rfc2217.html or at any number of other sites.

This mode opens an ACCES I/O eNET port when a TCP connection is established to the "local port". Port settings are embedded in data stream in accordance with RFC 2217.

Applications: UNIX systems and other platforms that have RFC 2217 Telnet capability can access and control the serial COM port of the ACCES I/O eNET.



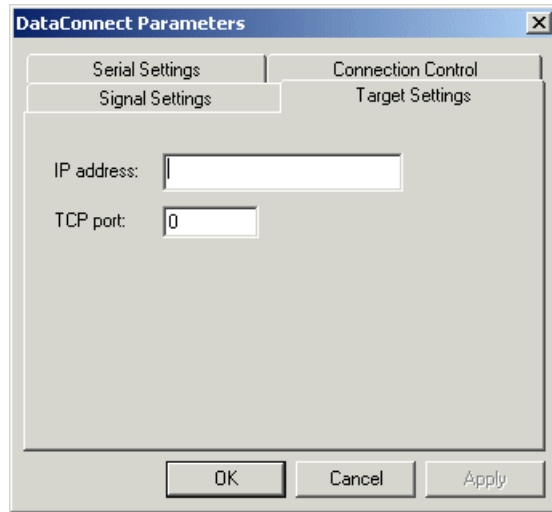
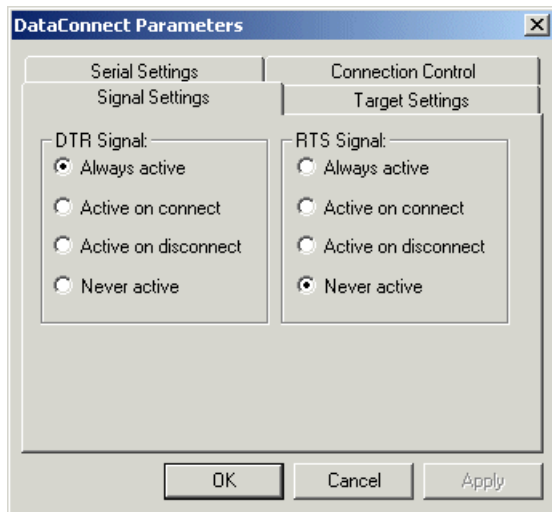
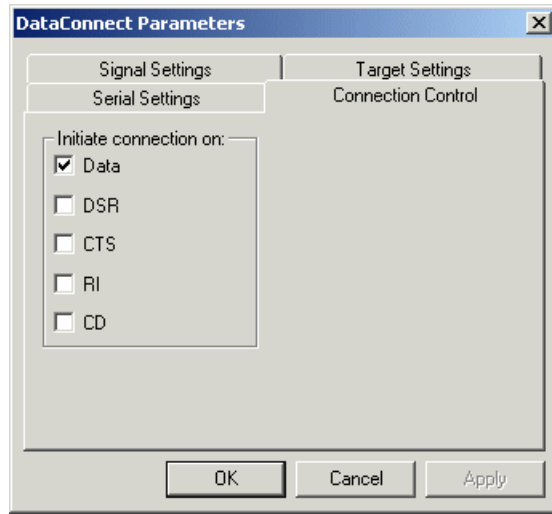
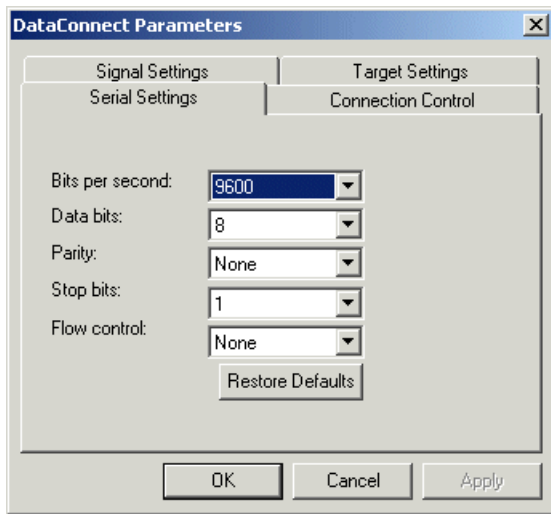
Data Connect Mode

Data Connect mode combines Raw Client mode and Raw Server Mode. In this mode, the ACCES I/O eNET will either initiate a TCP connection when activity is detected at the serial port, or it will receive TCP packetized serial data from the network port when an outside client connects to it.

The configuration parameters for this mode combine all the parameters found in Raw Client and Raw Server modes (see above for details).

With two ACCES I/O eNETs in this mode placed "back to back," the connection between them becomes in effect a cable extender over an Ethernet connection.

Applications: Data connect mode provides a serial-to-serial communication link that would not be practicable to implement as a directly-wired link; it can replace serial cables with an Ethernet connection.



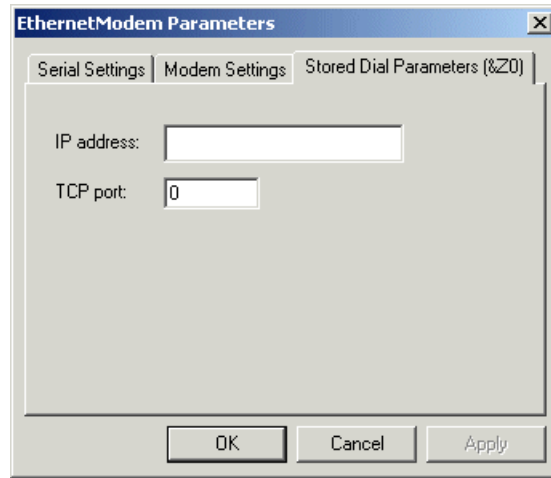
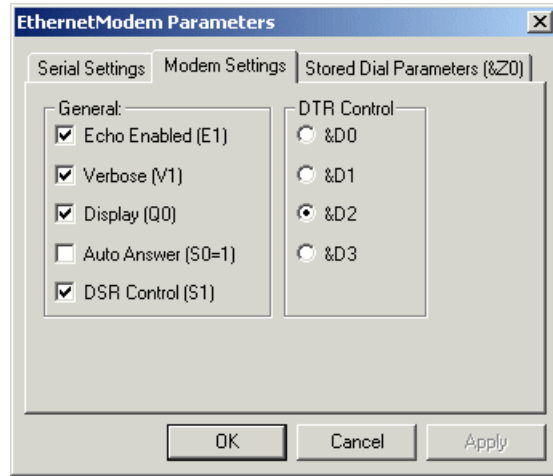
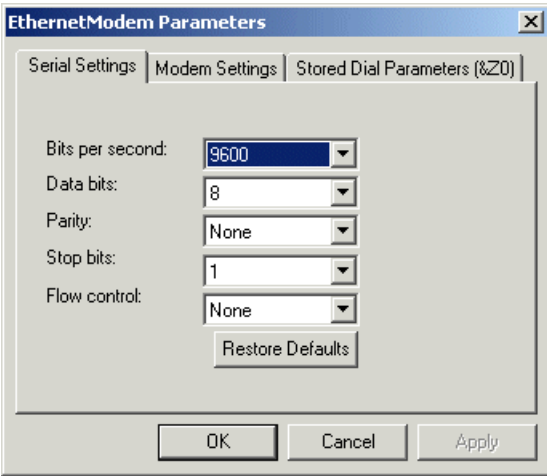
Ethernet Modem Mode

This mode allows Data Terminal Equipment (DTE) to control the ACCES I/O eNET using the conventional modem "AT" command set. In this mode, a DTE user is able to "dial" an IP address and TCP port. Incoming TCP connections are handled under AT command set rules.

The standard serial port settings for bits per second, data bits, parity, stop bits, and flow control are available for configuration, and should be set to match the DTE.

Modem settings include ECHO Enabled (E1), Result Codes Format Verbose (V1), Result Codes Display Return (Q0), Auto answer (S0=1), DSR Control (&S1). Modem DTR control can be set to &D0, &D1, &D2, or &D3.

Applications: To provide the standard "AT" command interface to user applications that wish to communicate with devices in an Ethernet environment. Remote console management that looks for AT interfacing can use this application.



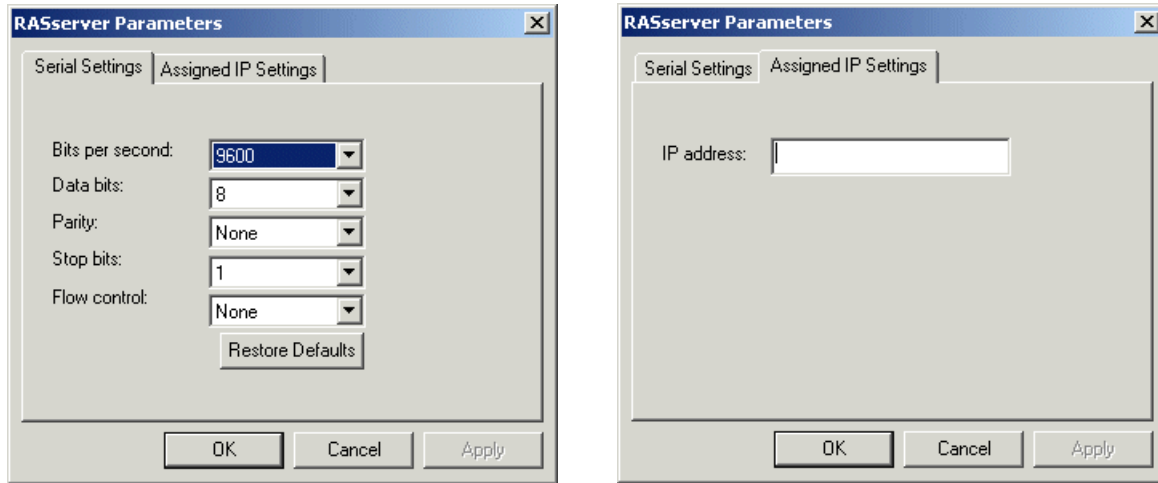
RAS Server Mode

Windows-based devices that have Remote Access Services (RAS) client capability but are not equipped with a direct network interface can access the network through a serial port using the Point-to-Point Protocol (PPP).

The serial port of the RAS client device is attached to the serial port of the ACCES I/O eNET, configured in RAS Server mode. The RAS negotiations are conducted between the RAS client and the ACCES I/O eNET RAS server.

In the initial negotiations between the RAS client and the ACCES I/O eNET, an IP address (configured by user) is assigned to the RAS client, which is used for all Ethernet communications related to the RAS client.

Applications: Windows CE embedded systems, Palm type units, or other portable data acquisition devices that may need access to a TCP/IP-Ethernet environment, and have PPP capability, but do not have an Ethernet port, can be connected to the serial port of an ACCES I/O eNET.

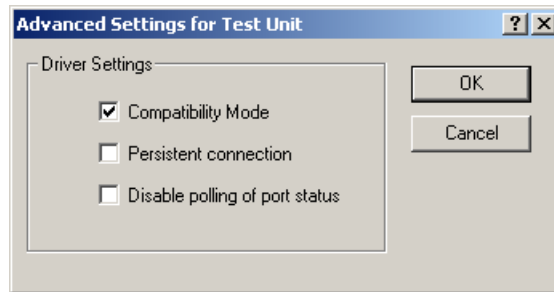


Disabled Mode

This mode simply disables a port; it has no configuration settings.

2. Virtual port (driver) settings

The ACCES I/O eNET virtual port allows a serial port on an ACCES I/O eNET to be used in same manner as a local serial port when the port is configured in Driver Mode (described above). In this state, the driver for the virtual port converts local serial port accesses into TCP/IP packets to be exchanged with ACCES I/O eNET ports.



Compatibility Mode

The ACCES I/O eNET virtual port normally operates in high performance mode. Compatibility mode supports applications that require a more accurate simulation of a local serial port. The need for Compatibility mode is indicated when data being sent to the remote serial port is lost or sent repeatedly.

Persistent connection

This setting maintains a persistent connection when the client station's connection is broken to the unit, then re-established. This setting is accessed through Window's Device Manager | Ports (COM & LPT).

Disable polling of port status

Polling of port status can be disabled. This is useful when a software application accessing the remote serial port repeatedly polls to check port status, slowing access to the remote port. This setting is accessed through Window's Device Manager | Ports (COM & LPT).

3. Virtual port (driver) bindings

Background

Activating an ACCES I/O eNET port in effect creates a "virtual" driver port that is associated with a particular physical serial port on a particular ACCES I/O eNET. When a driver virtual port is opened, a connection must be established to the appropriate ACCES I/O eNET. In normal operation, that connection is made to the IP address assigned to the ACCES I/O eNET at the time the activation was created. However, on many Ethernet/IP networks, the IP address of individual devices may change (for example, when a DHCP server assigns addresses). This address reassignment will cause virtual ports to fail or make unintended connections to unintended ACCES I/O eNETs.

Therefore, ACCES I/O eNETs are designed with the ability to "find" an ACCES I/O eNET port based on a "binding". A port binding is a network identification of the target ACCES I/O eNET that must match before a driver port will initiate a connection. Bindings may be made to the MAC address, Name, or IP address of the associated device.

Binding to MAC Address

MAC addresses are unique and permanent identifiers for Ethernet devices, and are assigned to devices when they are manufactured. Binding to an ACCES I/O eNET's MAC address ensures that a virtual port always makes a connection to that same physical device, even if the device's IP address or Name have changed. Binding to MAC address provides security and reliability. Virtual ports will only connect to that single particular physical device.

Binding to Name

Device Name is a 15-character field assigned by the ACCES I/O eNET system administrator. Binding a virtual port to a device's Name will ensure that a connection will be made to an actual port if a device can be found with the name specified in the "Bindings" dialog box. This port may be on a different physical device from the one with which the virtual port was initially communicating (that is, a device with a different MAC address), or it may be a port on the same physical device but with a changed IP address, or both. Binding to a device's Name provides reliability and dynamic connections. Virtual ports will connect to the device with a name that matches the binding. If a particular device is replaced with a new one with the same assigned Name, the virtual port will establish the connection. Also, Names can be reassigned at any time to cause client PCs to connect to new devices without being reconfigured.

Binding a virtual port to a Name allows that virtual port to be identified on the network with a more representative mnemonic than an IP address or MAC address. For example, a security system might name its virtual port targets "Camera1", "Camera2", "CardReader6", and so forth.

Binding to IP Address

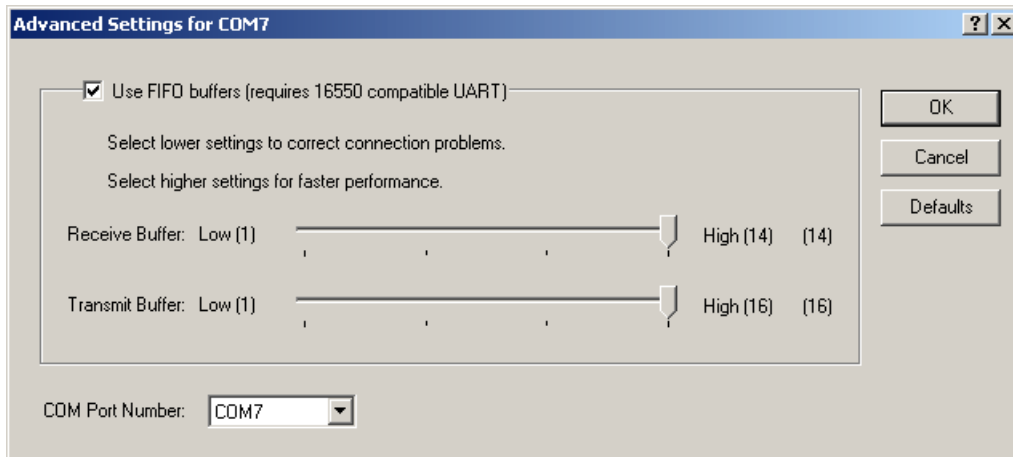
The IP address of a network device is assigned by either the ACCES I/O eNET system administrator or through a DHCP server. Binding a virtual port to an IP address will force that virtual port to attempt a connection to any device with that particular IP address only. Binding to IP address provides dynamic connections. Device IP addresses can be reassigned at any time to cause client PCs to form new connections without being reconfigured. Note: when no bindings have been stipulated, a virtual port is implicitly bound to an IP address because such an address is required to make a connection.

Binding to more than one parameter

Usually, only one degree of binding is sufficient for an individual virtual port to achieve the goals of robust communication and flexibility. It is however also possible to bind a virtual port to more than one parameter. Doing so requires careful consideration of the implications of maintaining connectivity. If multiple bindings are selected for one port, *all* individual binding parameters must match for a connection to be made. For example, enabling both IP address and MAC address bindings for a virtual port would cause that virtual port to find a particular physical device by MAC address, but make a connection only if the device's IP address also matched the binding setting.

4. Virtual port COM number assignment

By default, an ACCES I/O eNET virtual serial port is assigned to the next available COM number when it is activated. This COM number assignment can be reassigned to any unused COM number from 1 to 256.



5. Transmit FIFO buffer configuration

Each serial port of an ACCES I/O eNET has a first-in first-out (FIFO) buffer for transmitting data and a FIFO buffer for receiving data.

Transmit FIFO buffers are configurable and can buffer from 1 to 16 characters in the UART, for output to the serial port. Receive FIFO buffer levels are fixed at 8 characters.

Some serial devices, when they are not able to accept data from the serial port, will send an XOFF character to that port. Upon receipt of the XOFF character, the an ACCES I/O eNET will output the remaining characters in the port's transmit FIFO buffer. The an ACCES I/O eNET will then only accept more characters from the PC driver after an XON has been issued by the serial device.

If the nature of a serial device is such that it cannot accept buffered characters after sending an XOFF character, the user of an ACCES I/O eNET can set the transmit buffer level to some low value such as 1 or 2 characters, to overcome the situation where data is sent to a device that is unable to accept it. This may be necessary for POS printers and some CNC devices or PLCs, for example.

The transmit FIFO buffer level can be set using either the *eNET-Manager* (Port Settings | Advanced), or the Telnet configuration interface.

6. WAN Port configuration

Enter the IP address and TCP port number for WAN port configuration using this feature. Ensure that the IP address does not conflict with an IP address also in use on the local area network.