

TECHNICAL NOTE

Maple Model(s)

HMI Series
cMT Series

Title

Dual Ethernet Models

TN5110

P/N: 0907-5110

Rev. 02 Date:02/10/2019



Summary

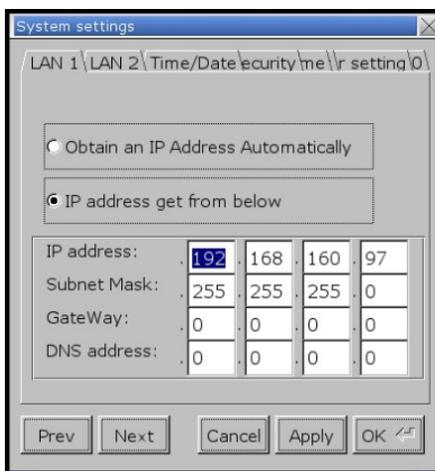
Dual Ethernet HMIs can be configured on two Local Area Networks (LAN) simultaneously. This technical note discusses the features available on our Dual Ethernet models and how to configure them. It also discusses best practices when exposing data from an industrial control system to the Internet.

Solution

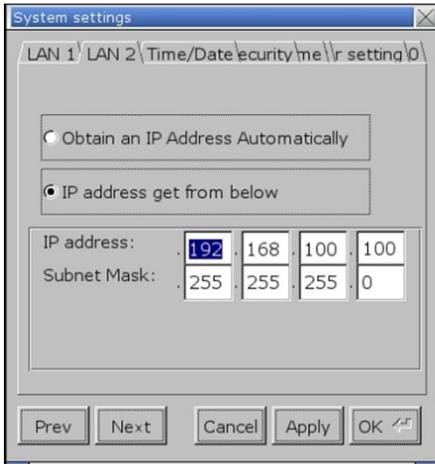
Configuring the Ethernet Ports on Advanced Series HMIs

The Ethernet ports on the Dual Ethernet model are configured via the system settings menu on the HMI hardware. This is the same process used to configure the Ethernet ports on other HMI models, except there is a separate tab in the system setting window for each port. The labels on the System Settings tab correspond to the labels on the Ethernet connectors on the back of the HMI. To configure the ports:

1. Apply power to the HMI.
2. Press the arrow icon in the bottom right hand corner of the touch screen.
3. Select the Gear icon to enter the system settings dialog. Enter the password (default is 111111).
4. Locate the LAN1 tab and configure the settings for LAN1. Click *Apply* to save the settings:



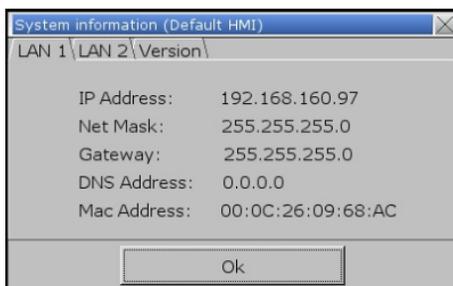
5. Locate the LAN2 tab to configure the settings for LAN2. Click *Apply* to save the settings:



LAN1 is the WAN port with settings for a DNS and Default Gateway. Use LAN1 for remote connections, use LAN2 for the local control network.

LAN1 and LAN2 must be configured on separate subnets. This means that the portion of the IP address masked by the subnet mask must be a unique number for each port. Devices configured on LAN1 cannot directly communicate with device on LAN2, refer to the [Communication Across Ethernet Ports](#) section below for more information.

The current settings for each port can be viewed in the information window, also accessed via the Arrow button in the bottom right hand corner of the HMI screen:



EBPro projects can be uploaded / downloaded on either port. The PC used to download the project must be configured with an IP address on the same subnet as the LAN port to which it is connected. See Technical Note 5077 (IP Addresses of an HMI and a PC), or your PC's documentation for information on setting the IP address of the PC.

Configuring Device Drivers

Devices such as PLCs, Drives, RTUs etc. can be configured on either port, however the preferred port is LAN2 which is intended to be reserved for the local control network. The device must be assigned a static IP address on the LAN to which it is attached. Multiple devices can be configured on a given LAN port with the use of an Ethernet switch.

Devices are added to the EBPro project by creating entries in the Device List (*Edit >System Parameters...* then go to the device tab of the *System Parameter Settings* window). The IP address assigned to the Device will be entered in the Device Properties window. This determines which Ethernet port is used by the device.

For information on the settings for any particular PLC, refer to the Controller Information Sheet (CIS) for that device. These are available for download from the Support Center at www.maplesystems.com/supportcenter/

Safety and Security Considerations

When the HMI is used as a gateway into the industrial control network, care must be taken so security and safety are not compromised. PLCs and drives control heavy, expensive equipment, often moving at high speed and high energy. Just because the HMI lets you expose complete control of these systems to the internet does not mean that is a good idea. A remote operator can only see what is presented to them via the HMI project. EBPro provides a number of security mechanisms. When adding remote access to a control system follow these guidelines:

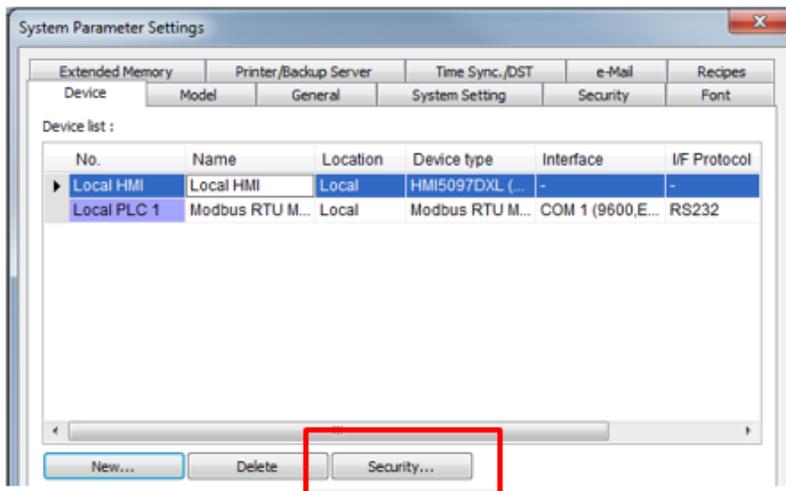
- Always provide mechanisms for local control / shut down – Machines that can present a safety concern should always be adequately staffed on site. A mechanical means of disconnecting any source of energy and returning the system to a safe condition should always be made available to the local operator.
- Default to less access – If there is not a compelling reason to allow remote access, disable those features.
- Use read only access whenever possible – A great deal of utility can be added to a system by knowing what it is doing without being able to control it. If remote control is not needed and could present a safety risk, disable it.
- Use the security features provided – Change passwords from the defaults and store in a safe place. Disable remote write access if it is not needed.
- Restrict access to personnel that need it - Use passwords for access to project files, access to VNC, and the project security features. Update projects regularly and change access when it is no longer needed.

Local Security

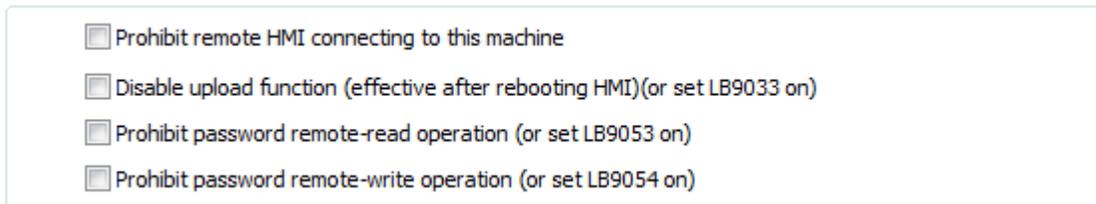
The arrow icon that appears (by default) in the bottom right corner of the HMI screen provides access to the HMI's local settings. The default password (111111) should be changed to restrict local access to these settings. This password protects the VNC password, enable / disable option, project upload / download passwords and many other settings. The arrow can be disabled in the project.

Data Security

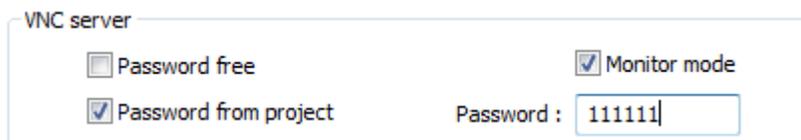
Access to data in the HMI can be restricted by a range of addresses or by read / write access. Notification of attempted access to protected data can trigger an alarm. To configure data security settings click on the *security* button for the Local HMI entry in the *Device List*.



In addition the *System Settings* or *Remote* tab of the *System Parameter Settings* window contains several options to restrict remote access to HMI data:



The VNC server password can be set on this tab:



Setting a password here will override any password entered from the HMI screen. If the password will need to be updated, deselect this option.

The *Monitor mode* option will allow the VNC client to display the application but the HMI will not accept any input from the client.

For more information on these options refer to the section on configuring the System Parameter Settings in the *EBPro Programming Manual*.

EBPro Security Feature

The EBPro security feature contains many tools to restrict access to HMI screens, objects and functions. There are tools to manage passwords at run time, add users, update passwords and access levels, and create temporary users. Refer to the security chapter in the *EBPro Programming Manual* for a complete discussion of the security feature.

When using VNC, be aware that the remote user will have the same security level as the local operator.

Project Security

Restricting access to the EBPro project file protects not only access to the function of the HMI but also the intellectual property that the project represents. EBPro has many ways to protect the project file:

- Disable or password protect project upload from the HMI
- Disable or password protect de-compilation of the project file
- Password protect the project file itself.

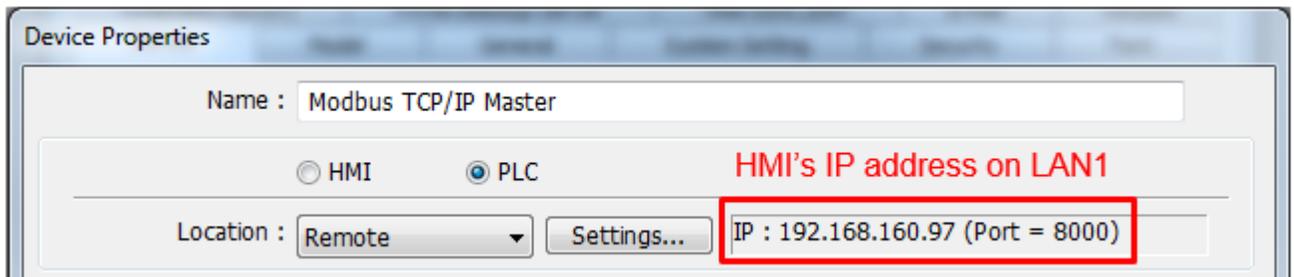
These features are also discussed in the Security chapter of the *EBPro Programming Manual*.

Communication Across Ethernet Ports

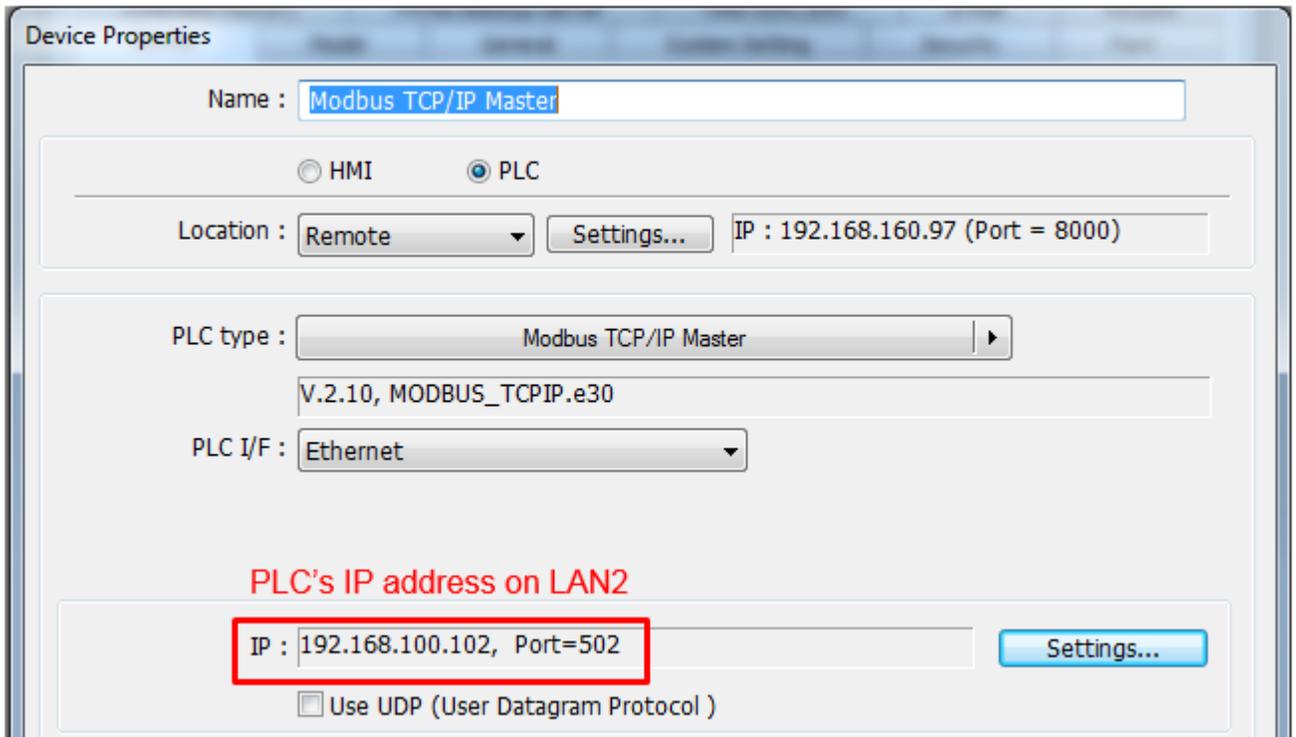
Because LAN1 and LAN2 must be configured to use different subnets, devices configured on LAN1 cannot communicate directly with devices on LAN2. For example if PLC1 is connect to LAN1 and PLC2 is connected to LAN2, PLC1 cannot read a Modbus register in PLC2. However, the HMI application *can* be configured to move data between the two devices, for example using a data transfer object or a macro to read data from PLC1 on LAN1 and write to PLC2 on LAN2.

Similarly, an additional Graphic HMI configured on one of the LAN ports cannot directly access data in a PLC on the opposite LAN port. As a result, it is *not* possible to connect multiple Dual Ethernet HMIs in a Daisy Chain configuration and give them all access to data in a single PLC. The HMI project can, however, be configured to copy data from a PLC on one of the ports to a single HMI on the opposite port. Specifically, the Remote PLC feature can be used to add a single additional HMI on the second LAN port. This is done when configuring the PLC entry in the Device list of the second HMI. Follow these steps:

1. Set the *Location* of the PLC to *Remote*. Enter the IP address assigned to the Dual Ethernet HMI's LAN port. This is the IP address for the LAN port that the second HMI is directly connected to:



2. In the IP section of the *Device Properties* window, enter the IP address assigned to the PLC:



For further information on the Remote PLC feature refer to *Technical Note 5033 – Multiple HMIs connecting to one PLC*.