MATRIX SERIES

ETHERNET SERVICE GUIDE

Datalogic Automation Srl
Via S. Vitalino, 13
40012 - Lippo di Calderara di Reno
Bologna - Italy

Matrix Series Ethernet Service Guide

Ed.: 02/2008

06/12/07

CONTENTS

1 GENERAL DESCRIPTION 1
1.1 Introduction 1
1.2 Physical Networks 2
1.3 Protocol Stack 3
1.4 Data Exchange 7
1.5 Device Addressing And Identification 10
1.6 Socket 12

2 SETTING NETWORK COMMUNICATION 13
2.1 Using DHCP Client 14
2.2 Using Static IP Addressing 16
2.3 Using An Ethernet Crossover Cable 18
2.4 Remotely Managing a Reader 21

3 MATRIX NETWORK SERVICES 23
3.1 Data Socket 24
3.2 Image Socket 27
3.3 Image FTP Client 29
3.4 HTTP Server 31
3.5 E-mail Client 33

4 ETHERNET HARDWARE BASICS 35
4.1 Cabling 35
4.2 LAN System Components 38

1 GENERAL DESCRIPTION

1.1 INTRODUCTION

Ethernet is the most popular physical layer LAN technology in use today.

Ethernet was created by Xerox Corporation (in cooperation with DEC and Intel) in 1976. Ethernet uses a Bus or Star topology and supports data transfer rates from 10 Mbps to 100 Mbps.
The newest versions of Ethernet, called Gigabit Ethernet, support data rates from 1 to 10 Gigabits per second (1000 Mbps to 10000 Mbps).

Ethernet uses the CSMA/CD access method to handle simultaneous demands.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers (IEEE) defines the Ethernet standard as IEEE Standard 802.3.
This standard defines rules for configuring an Ethernet network as well as specifying how elements in an Ethernet network interact with one another.
By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

1.2 PHYSICAL NETWORKS

Standard 10 Mbps Ethernet (IEEE 802.3)

A networking standard that supports data transfer rates up to 10 Mbps. The most common physical networks are:

- **10Base-T** standard (or **Twisted Pair Ethernet**): uses Unshielded Twisted Pair (UTP) cables with maximum segment length of 100 meters in Star topography.
- **10Base-2** (or **Thinnet**): uses a string of RJ-58 coaxial cables with maximum segment length of 500 meters in Bus topography
- **10Base-5** (or **Thicknet**): uses a single 75Ω coaxial cable with maximum segment length of 500 meters in Bus topography
- **10Base-FL**: is a set of optical fiber media specifications, which define connectivity between devices. It allows Ethernet segments to be connected over long distances (max 1km point-to-point)

100 Mbps Ethernet or Fast Ethernet (IEEE 802.3u)

A networking standard that supports data transfer rates up to 100 Mbps.

- **100Base-T**: is a series of specifications based on the older Ethernet standard, which operates over normal-quality twisted-pair cables (100Base-T4), high-quality twisted-pair cables (100Base-TX) and fiber optic cables (100Base-FX) in a Star topology.
  The **100Base-TX** standard is the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Gigabit Ethernet (IEEE 802.3z/802.3ab)

This new version of Ethernet supports data transfer rates of 1 Gigabit (1000 Megabits) per second over twisted-pair cables and fiber optic cables.

10 Gigabit Ethernet (IEEE 802.3ae)

This new version of Ethernet supports data transfer rates of 10 Gigabits (10000 Megabits) per second over fiber optic cables.

Currently the most widely used version of Ethernet technology is the 10 Mbps Twisted Pair variety (10Base-T).
Matrix readers support 10Base-T and 100Base-T physical networks.

1.3 PROTOCOL STACK

The TCP/IP protocols enable communication between pairs of hosts, or 'peers', on a network. The **Protocol Stack** structure can be conceptualized as a series of layers or '**stack**', between an application and the physical network.

Each protocol layer on one peer has a corresponding layer on the other peer. To the application, it appears that it has a virtual connection to an application running on another host. In reality, data is passed over the network in the physical form that the network can handle.

Each layer is required, by design, to handle communications in a predetermined fashion. Each protocol formats communicated data and appends information to or removes information from the data. Then the protocol passes the data to a lower layer on the sending host or a higher layer on the receiving host.

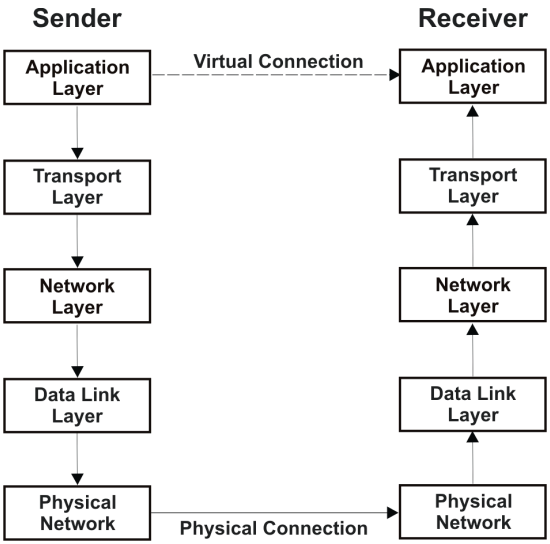


Figure 1 - Protocol Stack Scheme

Physical Network

The physical medium used to carry Ethernet signals between computers.
Ethernet signals are transmitted serially, one bit at a time, over the shared signal channel to every connected station.

Data Link Layer

This layer consists of:

- **Framing**: A station transmits its data in the form of an Ethernet Frame, or Packet
- **MAC**: Abbreviation of Medium Access Control.
  A set of rules embedded in the Ethernet interface located in each station, that allows multiple computers to fairly arbitrate access to the shared Ethernet channel. The Medium Access Control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**).
  This standard enables devices to detect a collision. After detecting a collision, a device waits a random delay time and then attempts to re-transmit the message. If the device detects a collision again, it waits twice as long to try to re-transmit the message. This is known as Exponential Back Off.

Network Layer

This layer is based on the Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level.
The following table represents the most popular and known protocols:

- **DHCP**: Abbreviation of Dynamic Host Configuration Protocol.
  A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.
  DHCP also supports a mix of static and dynamic IP addresses
- **IP**: Abbreviation of Internet Protocol version 4.
  Specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), which establishes a virtual connection between a destination and a source.

Transport Layer

This layer is based on one of the Internet transport Layer protocols, either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). These protocols use a set of rules to exchange messages with other stations at the information packet level.
The following table represents the most popular and known protocols:

- **TCP**: Abbreviation of Transmission Control Protocol.
  Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data.
  TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

- **UDP**: Abbreviation of User Datagram Protocol.
  A connectionless protocol that, like TCP, runs on top of IP networks.
  Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

Application Layer

This layer groups the Session, Presentation and Application layers.
Networking application programs send messages or streams of data to one of the Internet Transport Layer protocols.
The following table represents the most popular and known protocols:

- **DNS**: Abbreviation of Domain Name System (or Service).
  An Internet service that translates alphabetic domain names (e.g. www.datalogic.com) into IP addresses. Since the Internet is really based on IP addresses, every time you use a domain name, a DNS service must translate the name into the corresponding IP address.

- **FTP**: Abbreviation of File Transfer Protocol.
  It is a protocol used to upload files from a workstation to an FTP server or download files from an FTP server to a workstation.
  It is the way that files get transferred from one device to another in order for the files to be available on the Internet.

- **HTTP**: Abbreviation of Hypertext Transfer Protocol.

  This protocol defines how messages are formatted and transmitted, and what actions Web Servers and Browsers should take in response to various commands.

  For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web Server directing it to fetch and transmit the requested Web page.

  The terms HTTP Server and Web Server are interchangeable and mean the application using the HTTP protocol in charge of replying to the requests coming from a Client application (like Internet Explorer or Netscape).

- **POP3**: Abbreviation of Post Office Protocol version 3.

  A protocol used to recover e-mail from a Mail server. Most e-mail applications use the POP3 protocol, although some can use the newer IMAP4 (abbreviation of Internet Message Access Protocol version 4).

  This protocol can be used with or without SMTP.

- **SMTP**: Abbreviation of Simple Mail Transfer Protocol.

  A protocol for sending E-mail messages between servers. Most E-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

  In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP (or IMAP) server and the SMTP server when you configure your e-mail application.

- **Telnet**: TCP/IP Terminal Emulation Protocol.

  A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network.

1.4 DATA EXCHANGE

The following figure shows how each layer adds (or removes) header information to data traveling away from (or toward) the application layer.
The process of adding header information is termed **Encapsulation**; removing header information is termed **Decapsulation**.

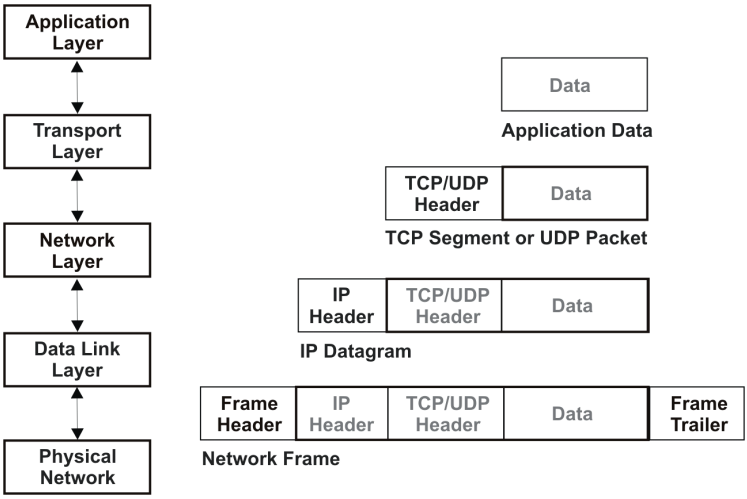


Figure 2 - Data Exchange Scheme

Encapsulation

Networking Application programs send messages or streams of data to one of the Internet Transport Layer protocols, either the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).
The Transport layer protocols receive the data from the application, divide it into smaller pieces called TCP segments or UDP packets, add a destination address, and then pass the packets down to the next protocol layer, the Network layer.
The Network layer encloses the packet in an Internet Protocol (IP) frame, adds the frame header, decides where to send the datagram (either directly to the destination system or indirectly via a router or gateway), and passes the datagram down to the Data Link layer.
The Data Link layer accepts IP datagrams, encapsulates them within frames that are specific to the network hardware such as Ethernet, Token-Ring or Fiber Distributed Data Interface (FDDI), and transmits these over the network.

Decapsulation

Frames received by a host are processed through the Protocol layers in the reverse order. Each layer strips off the corresponding header information, until the data ends up at the application layer.
Frames are received by the Data Link layer, which strips off the frame header and trailer, and sends the Datagram up to the Network layer.
The Network layer strips off the IP header and sends the packet up to the Transport layer.
The Transport layer strips off the TCP or UDP header and sends the data up to the networking Application programs.

The Internet Protocol (IP) defines addressing, routing, and data block handling over the network. The Transmission Control Protocol (TCP) assures that no data is lost or duplicated, and that everything sent to the connection arrives correctly at the target.

IP Frame Header

The Internet Protocol (IP) defines addressing, routing, and data block handling over the network. The Transmission Control Protocol (TCP) assures that no data is lost or duplicated, and that everything sent to the connection arrives correctly at the target.

The IP frame header contains routing information and control information associated with datagram delivery. It does it on the basis of an IP address (32 Bytes long).
IP implementations must accept at least packets of 576 bytes (maximum-size IP header is 64 bytes).

The IP header structure is as follows:

<table>
<tr><th>Bits
0-3</th><th>Bits
4-7</th><th>Bits
8-15</th><th colspan="2">Bits
16-31</th></tr>
<tr><td>Ver.</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragments Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Option + Padding</td></tr>
</table>

Figure 3 - IP Header structure

TCP Frame

TCP (defined by IETF RFC793) provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgment with retransmission of packets when necessary.
Virtual connection relies upon PORT concept: for each IP address 65536 ports are available. Some of them are dedicated to specific Application Layer Services (FTP, Telnet, etc.).

The TCP frame structure is as follows:

<table>
<tr><th colspan="8">Bits 0-15</th><th>Bits 16-31</th></tr>
<tr><td colspan="8">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="9">Sequence Number</td></tr>
<tr><td colspan="9">Acknowledgment Number</td></tr>
<tr><td>Offset</td><td colspan="2">Res.</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="9">Option + Padding</td></tr>
<tr><td colspan="9">Data</td></tr>
</table>

Figure 4 - TCP Frame structure

UDP Frame

UDP (defined by IETF RFC768) provides a simple, but reliable message service for transaction-oriented services.
Each UDP header carries both a source port identifier and destination port identifier, allowing high-level protocols to target specific applications and services among hosts (Sockets etc).

The UDP frame structure is shown as follows:

Bits 0-15	Bits 16-31
UDP Source Port	UDP Destination Port
UDP Message Length	UDP Checksum
Data	

Figure 5 - UDP Frame structure

1.5 DEVICE ADDRESSING AND IDENTIFICATION

Every device connected to a TCP/IP network is identified by a set of parameters, which manage the main system characteristics of the Ethernet communication.

- **IP Address**: Every device connected to a TCP/IP network must have a unique IP (Internet Protocol) address. This address is used to reference the specific device.

  Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods.

  Each number can be zero to 255. For example, 172.16.11.220 could be an IP address.

  The four numbers in an IP address are used in different ways to identify a particular network and a host on that network. Three regional Internet registries assign Internet addresses from the following three classes:

  - Class A: supports 16 million hosts on each of 127 networks.
  - Class B: supports 65,000 hosts on each of 16,000 networks.
  - Class C: supports 254 hosts on each of 2 million networks.

- **Subnet Mask**: A mask used to determine what subnet an IP address belongs to. An IP address has two components, the Network address and the Host address.

  For example, consider the IP address 172.16.11.220.

  Assuming this is part of a Class B network, the first two numbers (172.16) represent the Class B network address, and the second two numbers (11.220) identify a particular Host on this network.

  The related Subnet Mask is: 255.255.255.0.

  Note: Class A: 24 bits; Class B: 16 bits; Class C: 8 bits.

- **Gateway**: The Gateway address, or router, allows communication to other LAN segments. The Gateway address should be the IP address of the router connected to the same LAN segment.

  In enterprises, the Gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the Gateway is the ISP that connects the user to the Internet.

- **DNS Address**: The DNS is used to resolve alphabetic computer names.
  Consult your network administrator to obtain a new address. This information is necessary only if the name must be used instead of the IP address to set up an Ethernet service.

- **MAC Address**: Abbreviation of Media Access Control address
  It is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub layers:

  - Logical Link Control (LLC);
  - Media Access Control (MAC).

  The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.
  The Ethernet address is also referred to as the hardware address or the MAC address.

NOTE

The Ethernet (MAC) address is available on an externally visible label on the Matrix-21XX and on the Matrix 400-x00-010 reader models.

1.6 SOCKET

It represents a single virtual connection between two network applications. Two applications usually run on different computers and they can create multiple socket instances to communicate each other.

The virtual connection relies upon the Port concept: in TCP/IP and UDP/IP networks, a Port is an endpoint to a logical connection.
For each IP address 65536 ports are available. Some of them are dedicated to specific Application Layer Services (FTP, Telnet, etc.).

In order to identify both the location and application to which a particular packet is to be sent, IP Address (location) and Port Number (application) are combined into a functional address called Socket.

NOTE

Matrix family readers support one Data Socket for data transmission, one Image Socket for image files transmission and one System Socket (reserved for the VisiSet™ configuration tool and Host Mode programming).

Each Socket activated on the Matrix readers can be Client or Server:

Server

Matrix plays the passive role. It waits for connection from the Host (Client) side and can open a maximum of three clients simultaneously.
As soon as the Host (Client) starts the communication then the reader will send all the messages to the Host through the programmed Socket (IP Address + Port Number).
The Host can decide to close the communication at any time; normally in this case all further data transmitted by the Matrix Server device will be lost.

Client

Matrix plays the active role. It attempts a connection towards the Server as soon as it has something to send (a reading event occurs).
Data Exchange can be terminated by the Host Server application at any time. The Matrix Client device will re-attempt a new connection at the next reading event.

2 SETTING NETWORK COMMUNICATION

When using TCP/IP, the Matrix reader can use the Dynamic Host Configuration Protocol (DHCP) client service for dynamic IP addressing. It is also possible to configure the reader using a “static” IP address.

If a network connection is available, please consult your network administrator to verify the DHCP server availability within the network or to get a new static IP address.

It is possible to set up network communications:

- Using DHCP Client (refer to Paragraph 2.1).
- Using Static IP Addressing (refer to Paragraph 2.2)
- Using an Ethernet Crossover cable (refer to Paragraph 2.3).

Using the VisiSet™ configuration tool it is possible to access all the features and functionalities of the Matrix and monitor/control any reader on your Ethernet network (refer to Paragraph 2.4).

NOTE

If the Matrix Ethernet board is disabled, it is necessary to connect the reader using the serial communication port to enable it first.

2.1 USING DHCP CLIENT

Use the following procedure to set up communication on the Matrix when a DHCP server is available within your network:

1. Consult your network administrator to verify the DHCP server availability within the network.
2. Connect the Ethernet cable to the Matrix reader.
3. Connect the Auxiliary serial port of the reader to the PC and run the VisiSet™ configuration tool.
4. Select **Connect** to communicate with the reader.
5. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window will be displayed.
6. From the ETHERNET menu, enable the ETHERNET SYSTEM ***Status*** parameter (if previously disabled).
7. Enable the ***DHCP Client*** parameter (refer to Figure 6).

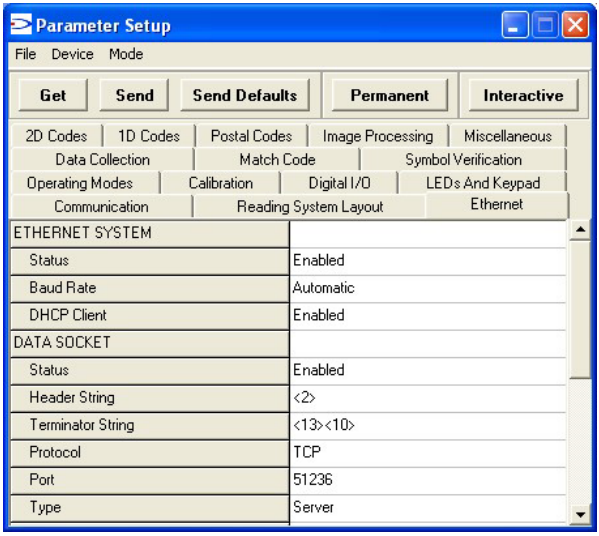


Figure 6 - Ethernet Board Configuration Window

8. Send the configuration to the permanent memory of the reader.
9. Verify that the COM LED on the top of the reader is blinking, which indicates Ethernet data activity.

10. Select **Connect** to communicate with the reader, the Ethernet board welcome message will be displayed (refer to Figure 7).

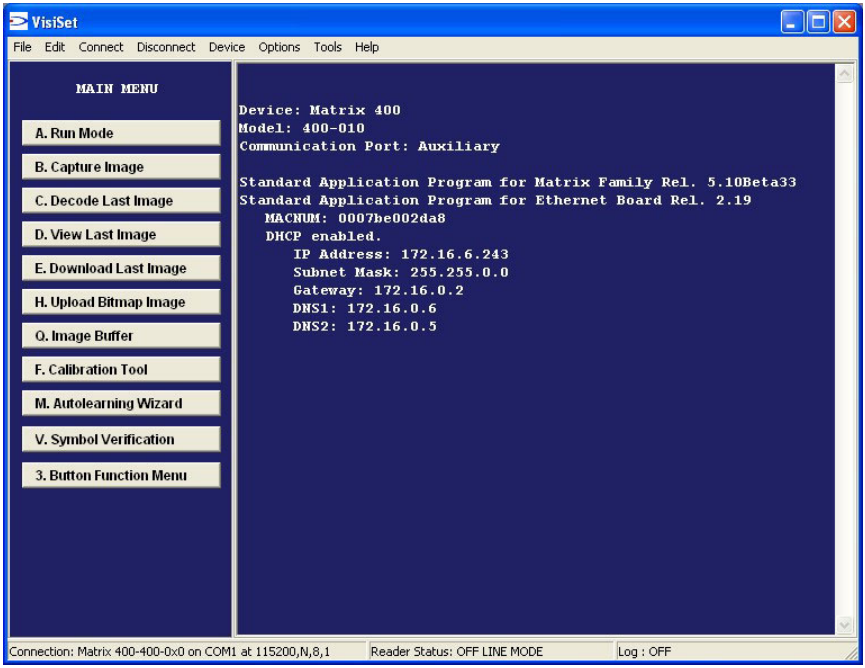


Figure 7 - VisiSet™ Main Window - Serial Communication

Now the Matrix is ready for use.

NOTE

The IP, Subnet Mask, Gateway, DNS1 and DNS2 addresses are dynamically and automatically set when using the DHCP client.

2.2 USING STATIC IP ADDRESSING

Use the following procedure to set up communication on the Matrix using static IP addressing:

1. Consult your network administrator to obtain a unique static IP address.
2. Connect the Ethernet cable to the Matrix reader.
3. Connect the Auxiliary serial port of the reader to a PC and run the VisiSet™ configuration tool.
4. Select **Connect** to communicate with the reader.
5. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window will be displayed.
6. From the ETHERNET menu, enable the ETHERNET SYSTEM ***Status*** parameter (if previously disabled).

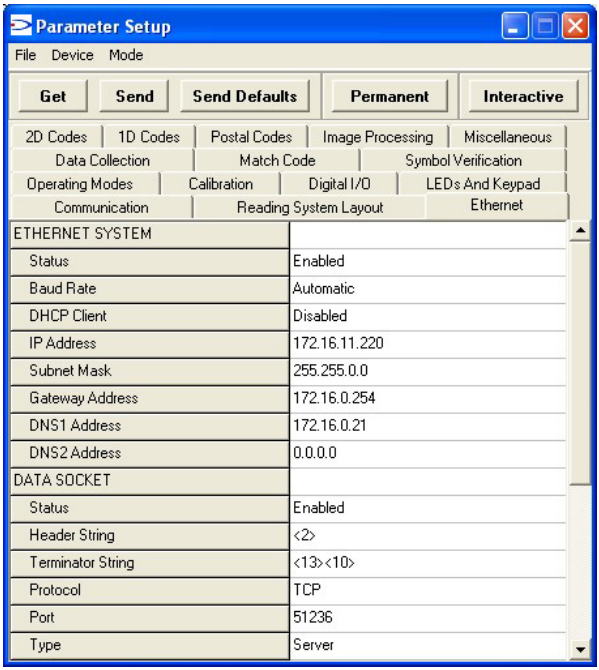


Figure 8 - Ethernet Board Configuration Window

7. In the ***IP Address*** field, enter the IP address provided by your network administrator (refer to Figure 8).
8. In the ***Subnet Mask*** field, enter the subnet mask provided by your network administrator (refer to Figure 8).
9. If your network administrator provided a Gateway address, enter it in the ***Gateway Address*** field; otherwise, leave it at 0.0.0.0 (refer to Figure 8).
10. If your network administrator provided a Domain Name Server address, enter it in the ***DNS1 Address*** field; otherwise, leave it at 0.0.0.0 (refer to Figure 8).
11. Send the configuration to the permanent memory of the reader.
12. Verify that the COM LED on the top of the reader is blinking, which indicates Ethernet data activity.
13. Select **Connect** to communicate with the reader, the Ethernet board welcome message will be displayed (refer to Figure 9).

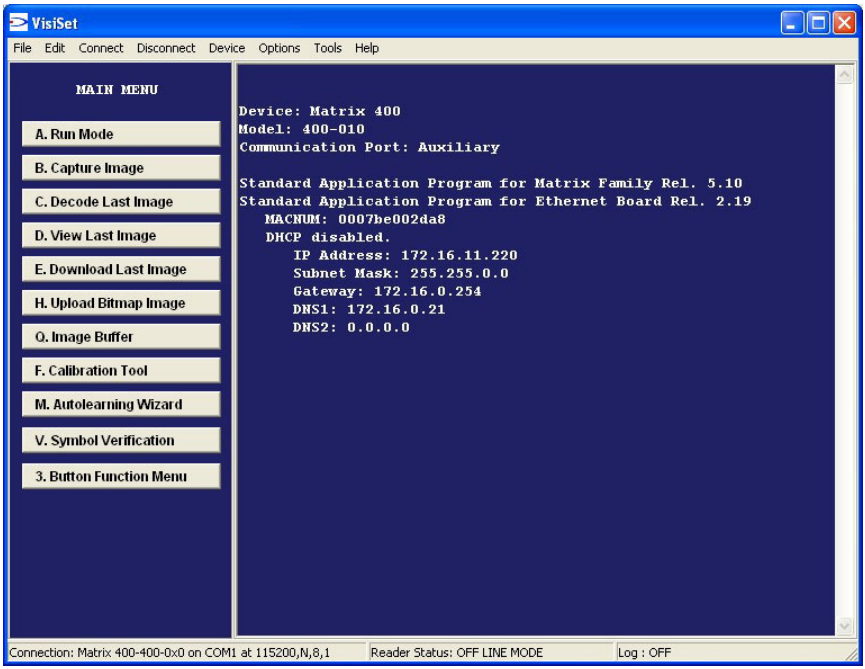


Figure 9 - VisiSet™ Main Window - Serial Communication

Now the Matrix is ready for use.

2.3 USING AN ETHERNET CROSSOVER CABLE

Use the following procedure to set up communication between a single Windows PC and a single Matrix reader using a crossover cable.

1. Log into the PC using an account with Administrator access rights.
2. Select Start, Settings, Control Panel.
3. Open the **Network** window (refer to Figure 10).

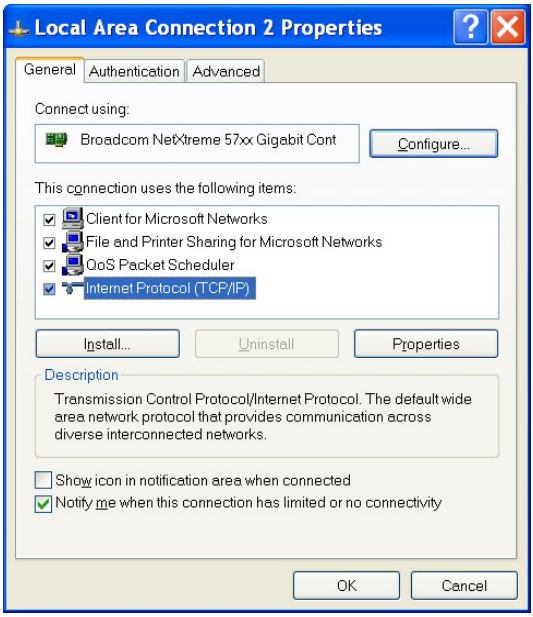


Figure 10 - Network Window

4. Select the **TCP/IP Protocol** option from the Protocols menu and click the **Properties** button.
5. Select the **Specify an IP Address** option, IP Address, Subnet Mask and Default Gateway fields will become active (refer to Figure 11).
6. It is advised to document your old settings before changing the TCP/IP properties of your PC.
7. In the IP Address field, enter the selected address (e.g. 172.16.11.210).
8. Replace the Subnet Mask with 255.255.0.0.
9. Remove any information in the Default Gateway field.

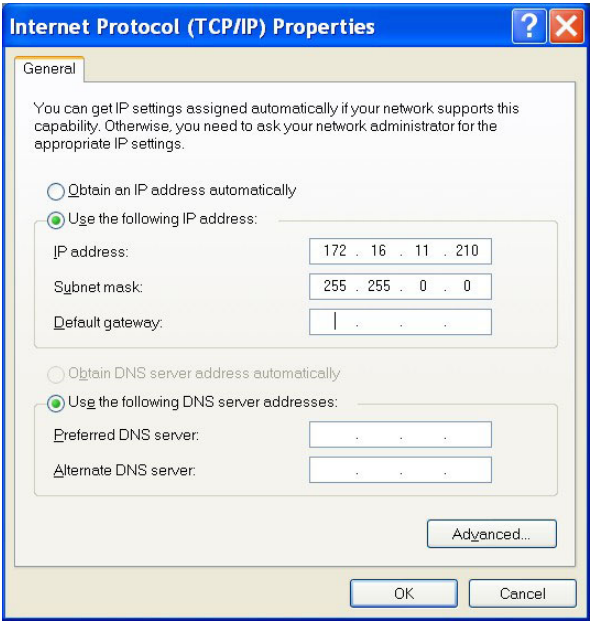


Figure 11 - TCP/IP Properties Window

Now the PC is ready for use.

NOTE

This procedure is referenced to a Windows XP PC. The screens will appear different with other Windows operating system versions.

10. Connect the Ethernet crossover cable between the PC and the Matrix reader.
11. Connect the Auxiliary serial port of the reader to the PC and run the VisiSet™ configuration tool.
12. Select **Connect** to communicate with the reader.
13. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.

14. From the ETHERNET menu, enable the ETHERNET SYSTEM ***Status*** parameter (if previously disabled).

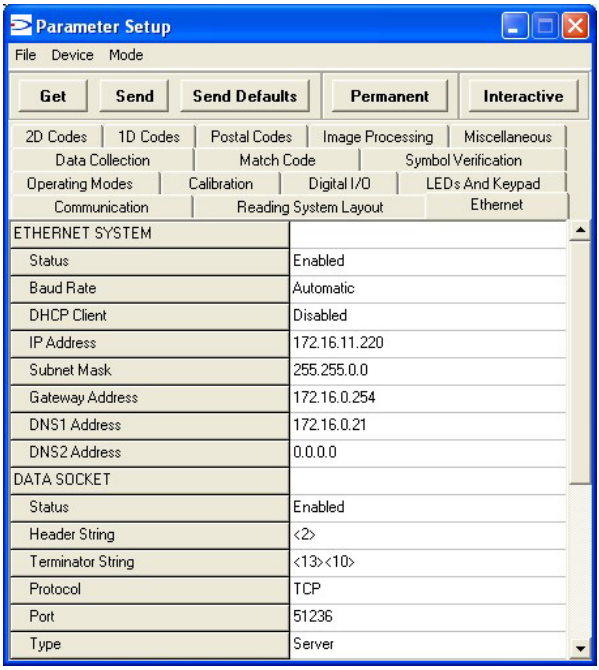


Figure 12 - Ethernet Board Configuration Window

15. In the ***IP Address*** field, enter the selected address (e.g. 172.16.11.220).
16. In the ***Subnet Mask*** field, specify 255.255.0.0.
17. Send the configuration to the permanent memory of the reader.
18. Verify that the COM LED on the top of the reader is blinking, which indicates Ethernet data activity.
19. Select **Connect** to communicate with the reader, the Ethernet board welcome message will be displayed (refer to Figure 9).

The PC and the Matrix can now communicate using the crossover cable.

2.4 REMOTELY MANAGING A READER

Use the following procedure to remotely manage a Matrix reader connected on your Local Area Network:

1. Connect the Ethernet cable to your PC and run the VisiSet™ configuration tool.
2. Select **Communication** from the **Options** menu.
3. Click **Ethernet** button, the Ethernet communication window will be displayed.
4. Click **Look for Devices on Network** button, VisiSet™ displays a list of Datalogic Ethernet devices that are currently on the network (refer to Figure 13).

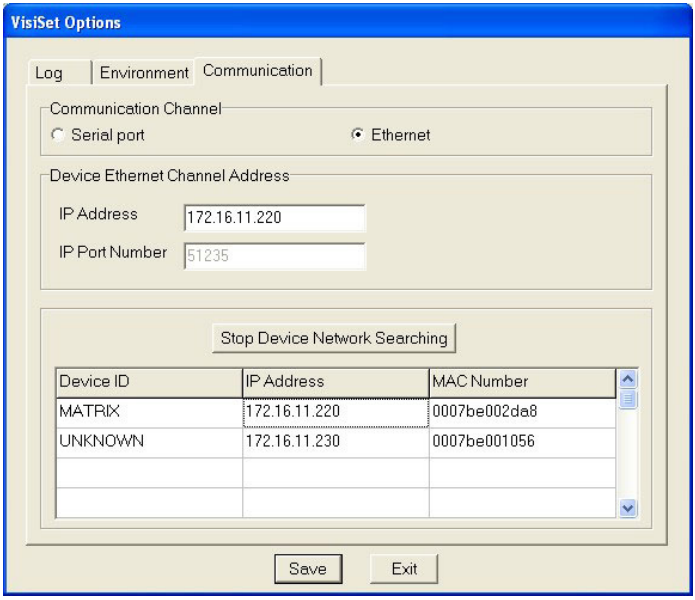


Figure 13 - Options - Ethernet Communication Window

5. Select the reader to be connected by double clicking on it, the address of the selected reader will be displayed in the **IP Address** field.
6. Select **Connect** to communicate with the reader, the Ethernet board welcome message will be displayed (refer to Figure 14).

The VisiSet™ welcome message indicates that the reader is connected and the connection is over the Ethernet communication channel.

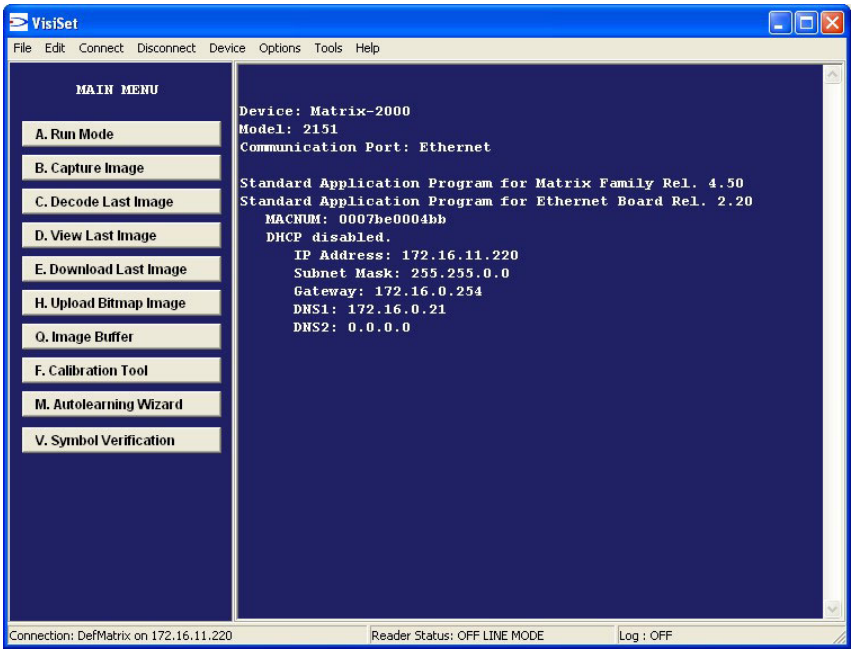


Figure 14 - VisiSet™ Main Window - Ethernet Communication

3 MATRIX NETWORK SERVICES

On the Matrix Ethernet interface the following communication channels are available:

- Data Socket (refer to Paragraph 3.1)
- Image Socket (refer to Paragraph 3.2)
- Image FTP Client (refer to Paragraph 3.3)
- HTTP Server (refer to Paragraph 3.4)
- E-mail Client (refer to Paragraph 3.5)

This chapter describes how to set and verify the correct functioning of Matrix network services.

3.1 DATA SOCKET

It is a point-to-point bi-directional communication channel available for the Ethernet communication allowing only to transmit and to receive decoded data.
Use the following procedure to set up and test Data Socket network service.

1. Connect the Matrix reader to your PC and run the VisiSet™ configuration tool.
2. Select **Connect** to communicate with the reader.
3. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.

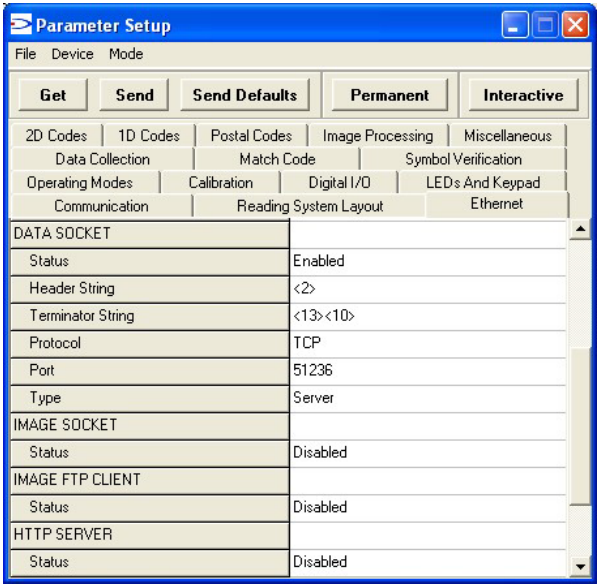


Figure 15 - Data Socket Configuration Window

4. From the ETHERNET menu, enable the DATA SOCKET ***Status*** parameter.
5. Set the other DATA SOCKET parameters as follows:

Header String: User Defined
Terminator String: User Defined
Protocol: TCP
Port: User Defined (e.g. *51236*)
Type: User Defined (*Client* or *Server*)

NOTE

Port numbers 51230, 51234, 51235, 65530 are reserved for the VisiSet™ configuration tool. It is strongly recommended not to use these numbers for the Data Socket network service.

6. In the ***Server Address*** field (only when the socket is configured as **Client**), enter the IP address or the alphabetic name of the PC on which the Server application program is running.
7. Send the configuration to the permanent memory of the reader.
8. Select **Disconnect** or **Run** to start the Matrix data transmission.

Use the following procedure to test Data Socket network service:

9. Log into your PC and run a TCP/IP (Winsock) connection using a standard terminal emulation program (like HyperTerminal) to simulate a Client or Server device.
10. In the Host Address field, enter the IP address of your Matrix reader (e.g. 172.16.11.200).
11. In the Port Number field, enter the Port Number selected for the Data Socket service (e.g. 51236).

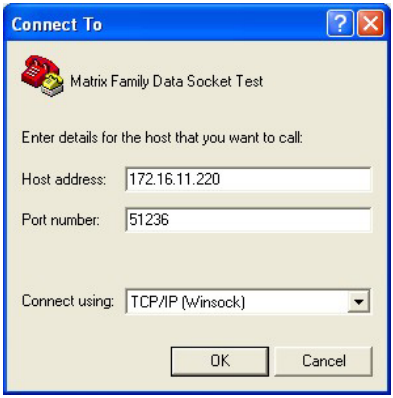


Figure 16 - HyperTerminal Connection window

12. Select Call option from the Call menu if the socket is configured as **Server** or select Wait For A Call option from the Call menu if the socket is configured as **Client** (refer to Figure 17).

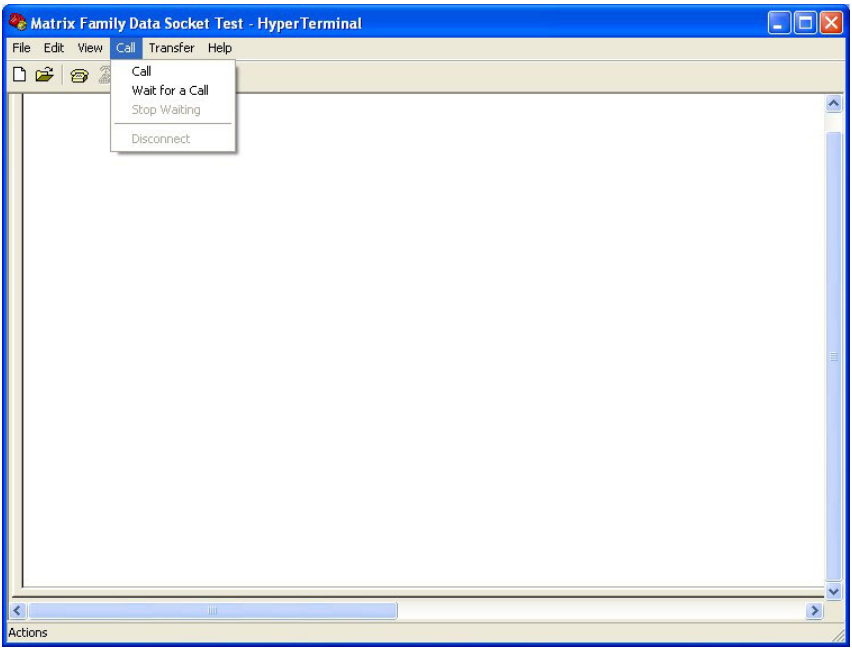


Figure 17 - HyperTerminal Call menu

Now the remote PC is ready for use.

When the terminal emulation program is launched it will detect and listen on the selected port. Verify the connection with the reader using the terminal emulator to display transmitted data.

3.2 IMAGE SOCKET

Image Socket is a point-to-point bi-directional communication channel available for Ethernet communication allowing to transmit image files only.

When transmitted, the image buffer is preceded by a header (refer to Figure 18):

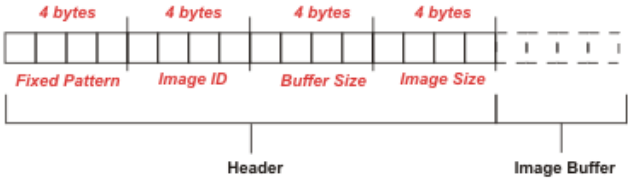


Figure 18 - Image Header Structure

- A fixed 4-byte pattern: 0xab, 0xcb;0x12, 0x34;
- A 4-byte image identification number, which is a progressive number;
- A 4-byte number giving the size of the image buffer;
- A 4-byte number giving the size of the image, where the first 2 bytes indicate the image columns while the last 2 bytes indicate the image lines.

Use the following procedure to set up the Image Socket network service.

1. Connect the Matrix reader to your PC and run the VisiSet™ configuration tool.
2. Select **Connect** to communicate with the reader.
3. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.
4. From the ETHERNET menu, enable the IMAGE SOCKET ***Status*** parameter (*On Successful Decoding*, *On Decoding Failure*, *Always Enabled*).
5. Set the other IMAGE SOCKET parameters as follows:

Image Subsampling:	User Defined
Image Format:	User Defined (*BMP* or *JPG*)
JPG Quality (1-100):	User Defined
Protocol:	User Defined (*TCP* or *UDP*)
Port:	User Defined
Type:	User Defined (*Client* or *Server*)
Server Address:	User Defined

NOTE

Port numbers 51230, 51234, 51235, 65530 are reserved for the VisiSet™ configuration tool. It is strongly recommended not to use these numbers for the Image Socket network service.

6. In the ***Server Address*** field (only when the socket is configured as Client), enter the IP address or the alphabetic name of the PC on which the Server application program is running.
7. Send the configuration to the permanent memory of the reader.
8. Select **Disconnect** or **Run** to start the Matrix image file saving.

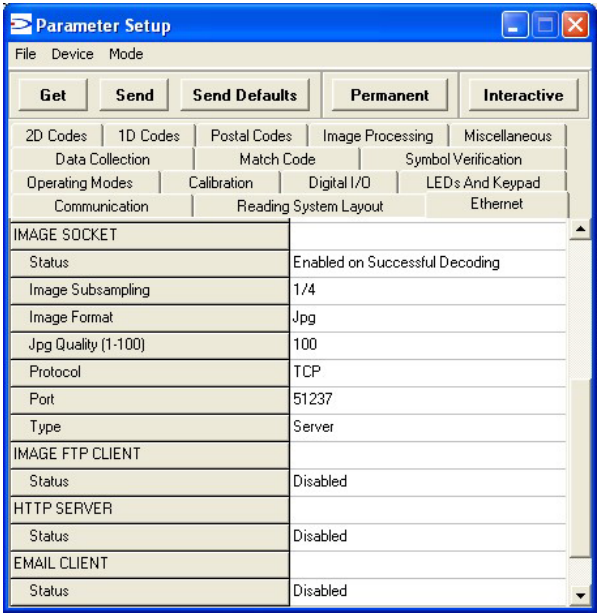


Figure 19 - Image Socket Configuration Window

3.3 IMAGE FTP CLIENT

The Image FTP Client is a high-level protocol channel available for Ethernet communication allowing to transmit images and save them to a file on a standard FTP server.
Use the following procedure to set up the Image FTP Client network service.

1. Log into your PC using an account with Administrator access rights and create the folder where the image files will be saved.
2. Run FTP Server program.
3. Create a new **User** profile entering your User name and your Password and add the folder where the image files will be saved to the FTP Server root.
4. Modify the permission settings of the folder where the image files will be saved (at least **Download** permission must be assigned).

Now the remote PC is ready for use. When the FTP Server is launched it will detect and listen to Port 21 of all available interfaces that it finds.

NOTE

*It is strongly recommended to disable the **Connection Timeout** parameter (if present in your FTP Server) to avoid connection losses.*

5. Connect the Matrix to your PC and run the VisiSet™ configuration tool.
6. Select **Connect** to communicate with the reader.
7. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.
8. From the ETHERNET menu, enable the IMAGE FTP CLIENT ***Status*** parameter (*On Successful Decoding*, *On Decoding Failure*, *Always Enabled*).
9. In the ***Server Address*** field, enter the IP address or the alphabetic name of the PC on which the FTP Server is running.
10. In the ***User Name*** field, enter the User name for your profile.
11. In the ***Password*** field, enter the Password selected for your profile.
12. In the ***Image Saving Path*** field, enter the path of the folder where the image files will be saved.
13. Set the other IMAGE FTP CLIENT parameters as follows:

Image Subsampling:	User Defined
Image Format:	User Defined (*BMP* or *JPG*)
JPG Quality (1-100):	User Defined
Image File Name:	User Defined
Max. Different Files to Save:	User Defined

14. Send the configuration to the permanent memory of the reader.
15. Select **Disconnect** or **Run** to start the Matrix image file saving.

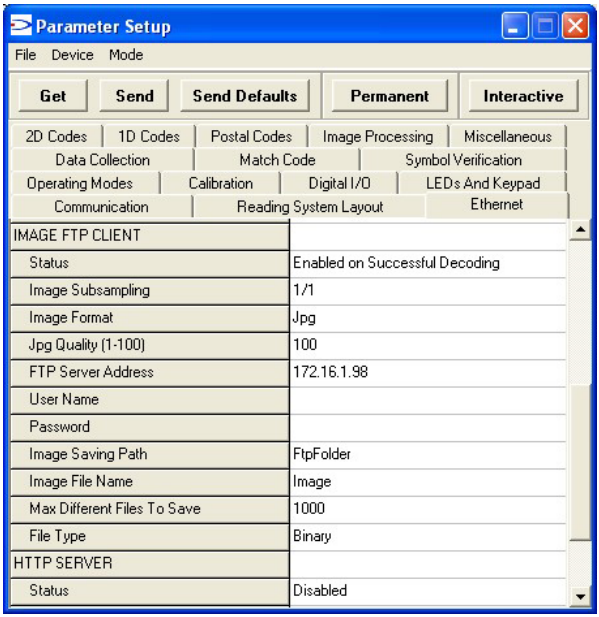


Figure 20 - Image FTP Client Configuration Window

3.4 HTTP SERVER

The HTTP server allows starting remote monitoring.
Remote monitoring allows checking the functioning of the reader via Ethernet. In particular, a remote monitoring PC can communicate with a Matrix reader by means of the Data Socket and Image Socket.

Use the following procedure to set up the HTTP Server network service.

1. Connect the Matrix reader to your PC and run the VisiSet™ configuration tool.
2. Select **Connect** to communicate with the reader.
3. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.

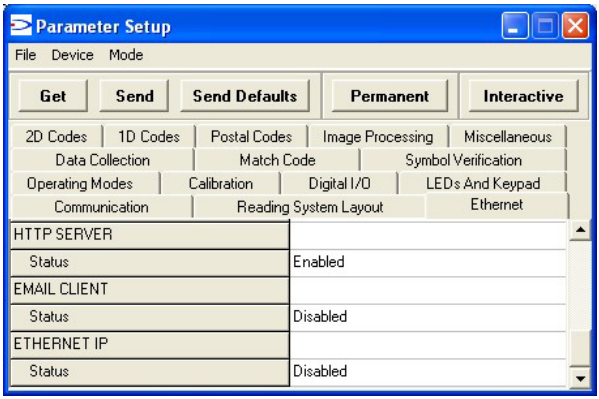


Figure 21 - HTTP Server Configuration Window

4. From the ETHERNET menu, enable the DATA SOCKET ***Status*** parameter.
5. Set the other DATA SOCKET parameters as follows:

Header String:	User Defined
Terminator String:	*<13><10>*
Protocol:	*TCP*
Port:	51236
Type:	*Server*

6. From the ETHERNET menu, enable the IMAGE SOCKET ***Status*** parameter (*On Successful Decoding*, *On Decoding Failure*, *Always Enabled*)

7. Set the other IMAGE SOCKET parameters as follows:

   Image Subsampling: User Defined
   Image Format: *JPG*
   JPG Quality (1-100): User Defined
   Protocol: *TCP*
   Port: 51237
   Type: *Server*

8. From the ETHERNET menu, enable the HTTP SERVER ***Status*** parameter.
9. Send the configuration to the permanent memory of the reader.
10. Select **Disconnect** or **Run** to start the Matrix Web page transmission.
11. Run a Web Browser on your PC (e.g. Microsoft Internet Explorer).
12. Select **Open** and enter the IP address of the reader to be connected, the monitoring Web page will appear on the screen showing a real-time image and data (refer to Figure 22).

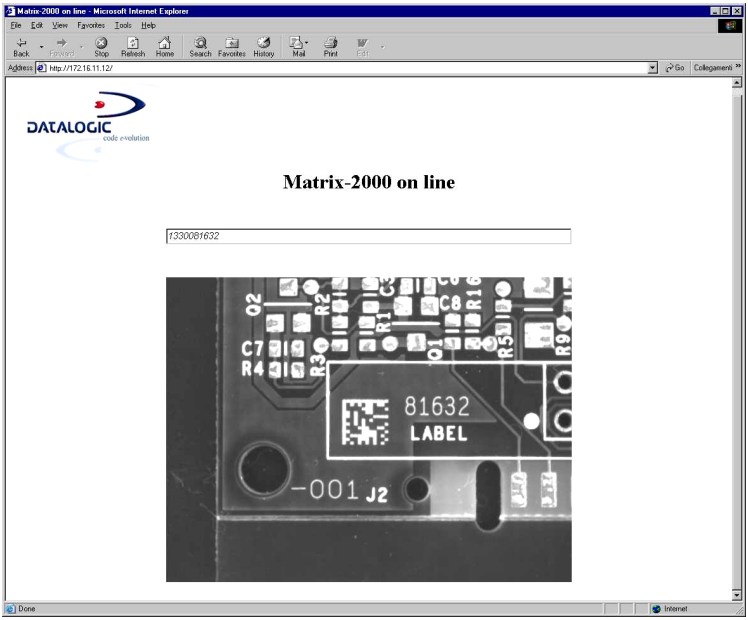


Figure 22 - Matrix-2000™ Web Page

3.5 E-MAIL CLIENT

Upon an #n number of occurrences of a specific event during an #m number of collections, the reader is able to automatically sends an e-mail message.

The e-mail message has the following format:

From: MACNUMBER@IPAddress
To: Addressee e-mail address (defined by the user)
Subject: Subject (defined by the user)
Text: Text (defined by the user)

Use the following procedure to set up E-mail Client network service.

1. Connect the Matrix reader to your PC and run the VisiSet™ configuration tool.
2. Select **Connect** to communicate with the reader.
3. Select **Get Configuration From Temporary Memory** from the **Device** menu, the Parameter Setup window menu will be displayed.

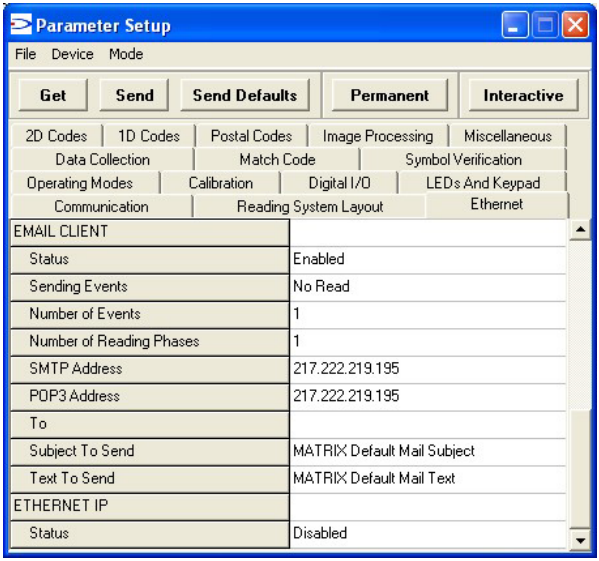


Figure 23 - E-mail Client Configuration Window

4. From the ETHERNET menu, enable the E-MAIL CLIENT ***Status*** parameter.
5. Set the other E-MAIL CLIENT parameters as follows:

Sending Events:	User Defined
Number of Events	User Defined
Number of Reading Phases	User Defined
To:	User Defined (e.g. example@it.datalogic.com)
Subject To Send:	User Defined
Text To Send:	User Defined

6. In the ***SMTP Address*** field, enter the Simple Mail Transfer Protocol address assigned by your network administrator.
7. In the ***POP3 Address*** field, enter the Post Office Protocol address assigned by your network administrator.
8. Send the configuration to the permanent memory of the reader.
9. Select **Disconnect** or **Run** to start the Matrix application program.

NOTE

*The length of the Addressee field (**To** parameter) is currently limited to 31 alphanumeric characters.*

4 ETHERNET HARDWARE BASICS

4.1 CABLING

ISO/OSI model uses acronyms to indicate a particular kind of physical layer (e.g. 10Base5, 10BaseT, 100Base, 10Broad36).

The first number (**1**, **10**, **100**, **1000**) indicates the transmission speed in Megabits per second.

The second term indicates the transmission type:

- **Broad**: Broadband (communication channel with a greater bandwidth and potentially capable of greater transmission rates)
- **Base**: Opposite of Broadband

The last number indicates the cable type:

- **2**: Coaxial cable with 0.25 inch diameter
- **5**: Coaxial cable with 0.50 inch diameter
- **T**: Twisted Pair cable
- **F**: Fiber cable
- **36**: Television type cable

The most used types of cabling for Standard Ethernet and Fast Ethernet are:

10BaseT (Standard Ethernet)

In 1990 IEEE approved 802.3i 10BaseT a completely new physical LAYER.

- 10BaseT uses two pairs of Unshielded Twisted Pair (UTP) telephone-type cable (one to transmit data and one to receive data) and RJ45 connectors according to EIA 568A and 568B specifications.
- The maximum length is 100m for each segment and the “4 repeater/5 segment” rule must be applied. So a 10BaseT LAN can have a maximum length of 500m.
- The physical topology of the standard is a Star, with nodes connected to a wiring hub or concentrator.
- Media has to be at least CAT3 (category 3) cabling, unshielded, voice grade telephone cable.
- Maximum Data Rate is 10 Mbps.

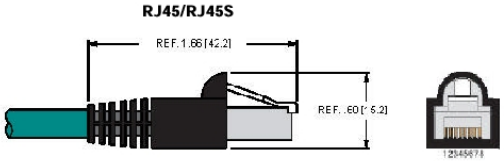
100BaseTX (Fast Ethernet)

IEEE standard is 802.3u: it is the extension of 10BaseT at 10 times the speed.

- 100Base-T uses two pairs of Unshielded Twisted Pair (UTP) Category 5 (100Ω impedance) or Type 1 Shielded Twisted Pair (STP – 150Ω impedance) cable (one pair to transmit data and one to receive data) and RJ45 connectors according to EIA 568A and 568B specifications.
- The maximum length is 100m for each segment and the "4 repeater/5 segment" rule must be applied. So a 100BaseTX LAN can have a maximum length of 500m.
- Media has to be CAT5 (Category 5) cabling.
- Maximum Data Rate is 100 Mbps.

An **RJ45 connector** is used in Twisted-Pair 10BaseT and 100BaseT Ethernet.

It is similar to a phone plug/jack but has eight pins. Looking at the plug (male) with the pins down, the pins are numbered from left to right 1 through 8.
Pin 1 and pin 2 are paired with each other, and pin 3 and pin 6 are paired with each other. The other pins (pins 4, 5, 7, and 8) are not used in Ethernet.



Contact Designation			
Pin No.	**TIA/EIA 568A**	**TIA/EIA 568B**	**Meaning**
1	White/Green	White/Orange	TX+
2	Green	Orange	TX-
3	White/Orange	White/Green	RX+
4	Blue	Blue	-
5	White/Blue	White/Blue	-
6	Orange	Green	RX-
7	White/Brown	White/Brown	-
8	Brown	Brown	-

Figure 24 - RJ45 Connector

The TIA/EIA-568A standard is supposed to be used in new network installations. Most of the Ethernet cables are still the TIA/EIA-568B standard; however, it makes absolutely no functional difference in which you choose.

Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections (refer to Figure 25).

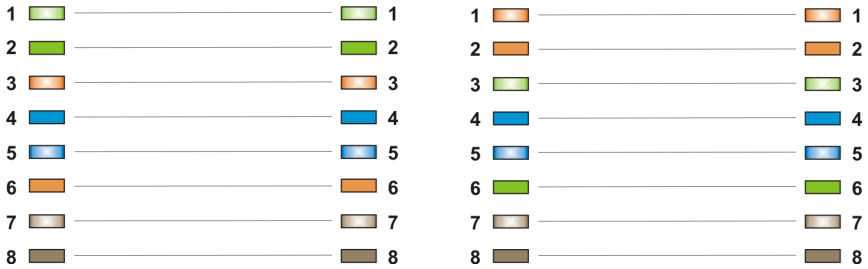


Figure 25 - EIA-568A and EIA-568B Straight-Through Cables

Two Ethernet stations can be directly attached to each other, but the cabling will be wired differently than a normal 10BASE-T Ethernet network connection. The 802.3 specifications refer to this direct connection between two stations as a Crossover cable (refer to Figure 26).

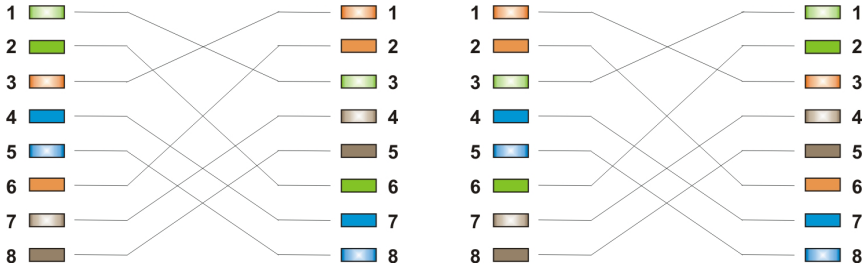


Figure 26 - EIA-568A and EIA-568B Crossover Cables

4.2 LAN SYSTEM COMPONENTS

Local Area Network (LAN) is a group of interconnected computers with the ability to share resources confined to a limited geographical area (typically about 3.000 m).

Different components could be present in a LAN depending on the topology; the following table represents the most popular and used components:

Repeaters

Repeaters are the simplest components that we can find in a network. It simply retransmits incoming electrical signals without considering any possible collisions.

Although repeaters are probably the cheapest way to extend a network, they do so without separating the collision domains, or network traffic. They simply extend the physical size of the network. All segments joined by repeaters therefore share the same bandwidth and collision domain.

Bridges

Bridges are used to connect two separate networks to form a single large continuous Local Area Network (LAN). The overall network, however, still remains one network with a single network ID (NetID).

The bridge only divides the network up into two segments, each with its own collision domain and each retaining its full bandwidth. All nodes on both sides of the bridge see the Broadcast transmissions.

The bridge exists as a node on each network and passes only valid messages across to destination addresses on the other network. Bridges can be used to extend the length of a network but in addition they improve network performance.

Hubs

Hubs are used to interconnect hosts in a physical star configuration.

All hosts connected to the hub share the available bandwidth since they all form part of the same collision domain.

A passive Hub serves simply as a conduit for the data, enabling it to go from one device (or segment) to another. So-called Intelligent Hubs include additional features that enable an administrator to monitor the traffic passing through the Hub and to configure each port in the Hub.

A third type of hub, called a Switching Hub, actually reads the destination address of each packet and then forwards the packet to the correct port.

Switches

Ethernet switches are expansion of the concept of bridging and are, in fact, intelligent (self-learning) multi-port bridges. Each port on the switch represents a separate segment with its own collision domain.
A typical use for a switch is a Backbone: for example, in a building we can have many PCs on several floors (different LANs). It's possible collect single LAN floor traffic with a hub and connect all the hubs with a switch.

Routers

Routers operate at the Network layer (level 3 of the ISO/OSI model). They forward packets to their destination, using the most direct available path.
A Router passes data packets using logical addresses and algorithms, which enable it to select the best route by which to transmit data packets based on the IP address.
In the Internet, a Router could be a hardware device or software, which defines the best route by which to reach the different nodes.

Gateways

Because routers are unable to connect LANs that are using different protocols, a Gateway is needed. A Gateway is a combination of hardware devices and software, which connects networks of different protocols.
It transmits data, which it has translated into a format that is compatible with the protocol used by other networks.
In enterprises, the gateway node often acts as a Proxy server and a Firewall. The gateway is also associated with both a Router, which uses headers and forwarding tables to determine where packets are sent, and a Switch, which provides the actual path for the packet in and out of the Gateway.