PART 2 – SOFTWARE

Contents

PART 2 – SOFTWARE 1

CONTENTS 3

INTRODUCTION 5

Minimum PC Specifications 5

IXP220 APPLICATIONS 7

IXP220 Modules 7

IXP220 Utilities 10

IXP220 NETWORK SPECIFICATIONS 13

Architecture 13

IXP220 Modules in a Network Environment 14

General Network Requirements 15

Running IXP220 across a LAN 16

Running IXP220 across a WAN 17

Properties Files 18

Configuring IXP220 Modules for a Stand-alone (Single PC) System 18

Configuring IXP220 Modules for a LAN (Firebird) 18

Configuring IXP220 Modules for a WAN 19

Using Routers Configuration 20

SYSTEM CONCEPTS 21

System Architecture Concepts 21

Sites 21

System Building Blocks 21

SOFTWARE INSTALLATION PROCEDURE 24

New IXP220 Installation 24

Installing the Database Server 25

IXP220 Installation Procedure 27

Install the USB Driver for the USB Registration Reader Interface 29

Upgrading an Existing Installation 30

PRE-CONFIGURATION PROCEDURE 31

RS485 Communications Infrastructure 31

USB Communications Infrastructure..... 31

TCP/IP Communications Infrastructure 31

Introduction

This Part of the manual provides an overview of the IXP220 System, and the basic steps required for software installation and pre-configuration.

Minimum PC Specifications

Consider a number of factors when determining the correct PC specifications for different scenarios:

- Number of Doors
- Number of Tagholders supported by the System
- Whether the Base Application and Firebird Database will reside on the same PC

Description	IXP220-1	IXP220-2	IXP220-3	IXP220-4
Description	Single APB Door or 2 non-APB Door System	4 APB Door System	256 APB Door System	Multi-site System (256 Doors per Site)
Processors A high performance model released within the last three months	1 Desktop Processor	1-2 Server Processor(s)	2 or more Server Processors	2 or more Server Processors
Free Memory Available for use by the Database Server only	1 GB	2 GB	4 GB	4 GB
Free Hard Disk Space Needed for Database storage, backups and archived copies	80 GB	160 GB	320 GB	320 GB
Display Monitor and graphics accelerator	1 024 x 768	1 024 x 768	1 024 x 768	1 024 x 768
Operating System Validated Operating System platforms	Microsoft Windows Server 2008 64-bit. Microsoft Windows 7 32-bit and 64-bit (Professional, Enterprise or Ultimate); Microsoft Windows Vista 32-bit ONLY (Business or Ultimate); Microsoft Windows XP 32-bit ONLY (Professional)	Microsoft Windows Server 2008 64-bit. Microsoft Windows 7 32-bit and 64-bit (Professional, Enterprise or Ultimate); Microsoft Windows Vista 32-bit ONLY (Business or Ultimate); Microsoft Windows XP 32-bit ONLY (Professional)	Microsoft Windows Server 2008 64-bit. Microsoft Windows 7 32-bit and 64-bit (Professional, Enterprise or Ultimate); Microsoft Windows Vista 32-bit ONLY (Business or Ultimate); Microsoft Windows XP 32-bit ONLY (Professional)	Microsoft Windows Server 2008 64-bit. Microsoft Windows 7 32-bit and 64-bit (Professional, Enterprise or Ultimate); Microsoft Windows Vista 32-bit ONLY (Business or Ultimate); Microsoft Windows XP 32-bit ONLY (Professional)

Description	IXP220-1	IXP220-2	IXP220-3	IXP220-4
Database Server Supported Database platforms	Firebird 2.1	Firebird 2.1	Firebird 2.1	Firebird 2.1

Table 1 – Minimum PC Specifications

The volume of transactions per Site affects the performance of the Database Server PC. Adjust the specification allowing for rapid Database growth and Reports that work with large result sets.

IXP220 Applications

The IXP220 Software incorporates a collection of Modules and Utilities. The Modules form the core of the IXP220 Suite and provide control for everyday and important functions. The Utilities provide support for advanced configuration and system maintenance. This section provides a brief description of IXP220's Modules and Utilities.

IXP220 Modules

Base Application Module

The Base Application is the communication, configuration and Tag enrollment module for the IXP220 Software. This user-friendly Module, allows for systematic installation and configuration of the System using wizards where possible.

The IXP220 Base Application performs a number of important functions including:

Communication

- Monitors the Database for edits made by for example, the Base Application and the Web Enrollment Module.
- Communicates details of all changes or edits made to the relevant Controllers.
- Polls the Controllers for transactions, then logs the transactions to the Database.
- Runs the web server.
- Opens socket connection ports for Modules such as ImproTouch (which make a direct connection to the Base Application).

Site and Host configuration

- **Auto-ID**—reports detected Hardware to the IXP220 System Software, and configures the Hardware for communication purposes.
- **Site Configuration**—allows configuration of your site.
- **Controller Configuration**—allows configuration of the installed Controllers.
- **Door Configuration**—allows configuration of the installed Terminals.
- **Access Group Configuration**—the key element of access control, this setting allows configuration of when (Access Time Patterns), and where (Areas) Tagholders have access.
- **Tagholder Configuration**—allows configuration of Tagholder details.
- **Holiday Configuration**—allows configuration of Holidays affecting your site.
- **Reason Code Configuration**—allows configuration of Reason Codes.
- **Message Configuration**—allows configuration of personalised messages.
- **Batch Tag Registration Configuration**—allows enrollment and configuration of batches of Tags.
- **Input and Output Devices Configuration**—allows configuration of Input and Output devices connected to your IXP220 System for use in Building Management.
- **Actions Configuration**—allows configuration of event driven or time triggered actions for use in Building Management.

The Base Application is a “scaled” software suite, therefore, features “unlock” based on the unlock codes (feature licences) purchased. The Base Application Unlock Code options include the following:

- Support for up to 256 doors
- Multiple Site support

Web Enrollment Module (General)

This Module requires an unlock (Web Tagholder Enrollment License) and has a maximum of 50 seats. It is intended for use by an operator using a PC at a location remote from the System’s Base Application (Host PC). This Module requires no extra IXP220 software installation, simply installing Java Runtime Environment V1.60 Update 20 or above allows any member of your staff (provided they have a valid username and password) access to the Module.

The Module’s basic function is enrolling Tags so **employee Tagholders** may access selected areas at named times. As this is an enrollment Module, each PC running the Module must connect to a Registration Reader. The benefit of running this now entirely web-based Module is less bandwidth usage promoting improved network speed. You may use the Web Enrollment Module with Windows® Internet Explorer 8 (and above) or alternatively Firefox 3 (and above).

Web Enrollment Module (Visitor)

This Module requires an unlock (Web Visitor Enrollment License) and has a maximum of 50 seats. It is intended for use by an operator using a PC at a location remote from the System’s Base Application (Host PC). This Module requires no extra IXP220 software installation, simply installing Java Runtime Environment V1.60 Update 20 or above allows any member of your staff (provided they have a valid username and password) access to the Module.

The Module’s basic function is enrolling Tags so **visitor Tagholders** may access selected areas at named times. As this is an enrollment Module, each PC running the Module must connect to a Registration Reader. The benefit of running this now entirely web-based Module is less bandwidth usage promoting improved network speed. You may use the Web Enrollment Module with Windows® Internet Explorer 8 (and above) or alternatively Firefox 3 (and above).

IXP220 Rich Client Module

The IXP220 Rich Client Module lets you configure Doors (Locations) and Tagholders from a separate PC (not running the IXP220 Base Application). In theory, you would use this Module where you need feature flexibility not offered by the Web Enrollment Module. These instances could include but are not limited to:

- During Biometric enrollment.
- Where you need to change Door (Location) configuration patterns (on a PC away from the Base Application) without stopping the IXP220 Base Application.

Tracker Module

The Tracker Module keeps you advised as to the whereabouts of selected Tagholders (maximum 10 Tagholders per site) as they move about the Site. Alternatively, you may use the

Tracker Module to monitor events at a selected Reader (maximum 10 Readers per Site). Both these facilities allow for better end user site management, by displaying the 20 transactions for today only, in time order per your group (Tagholders or Readers) selected.

*In instances where a single Tagholder (Reader) returns more transactions than others it may happen that some Tagholders (Readers) do not appear in the list of transactions. It must be emphasized that it is the **most recent 20 transactions for the group**, not the most recent for each individual Tagholder. Achieve best results with this Module by narrowing your range for monitoring to your exact requirements.*

On opening, the Tracker Module remains discreetly minimized as an icon in the System Tray (Notifications Area). As Tracker receives Tagholder transactions or events from Monitored Readers, notification pop-up windows display in the Notification area.

By default the Tracker Module refreshes every 10 seconds, this is the recommended setting. The refresh rate is, however, user configurable where you need a faster or slower refresh rate.

Visual Door Control Module

The Visual Door Control Module CCTV integration solution allows for better end user site management. In areas with rising crime, the operator can from a safe location monitor and control up to 4 Doors (Locations) (4 Cameras) at a time, per site.

The Module also allows tracking of up to 30 Tagholders at a time on a per site basis. The Tagholder monitor refreshes every 5 seconds giving you a near real time Tagholder tracking solution.

You may use the Visual Door Control Module with Windows® Internet Explorer 8 (and above) or alternatively Firefox 3 (and above). The Module is designed for use with the Axis 210 and 213D range of cameras.

ImproTouch Module

The ImproTouch Module requires an unlock (ImproTouch License) and has a maximum of 1 seat. This Module facilitates the integration and configuration of various third-party Biometric Readers for use with the IXP220 Software. These systems currently include various Sagem Fingerprint Readers integrated with the IXP220 Software via the Biometric Server Software. The Server Software also allows for the direct enrollment (registration) of Tagholders and related biometric data at those Biometric Readers from within the IXP220 Software.

The introduction of biometric access control greatly increases the access control capabilities of IXP220 Systems where you need extra security measures.

Card Designer Module

The Card Designer Module requires an unlock (Card Designer License) and has a maximum of 1 seat. This Module lets you design templates for use with Credit Card Tags. These templates can then be used to print information on to these Tags, such as company name, Tagholder's name, ID number, employee number, department, barcode, and so on, as well as a photograph of the Tagholder.

Web Reports Module

The IXP220 Software lets you compile Reports on functions and transactions within the IXP220 System. As these Reports are essentially Web Reports, so you can compile Reports for one or more Sites over LAN or WAN networks. The Reports Software allows selection of single or multiple Sites, allowing management of both.

Filters readily displayed on the screen, let you select parameters for running your Report. These filters may consist of information fields (occasionally), drop-down menus, checkboxes or calendars.

Webstore Module

The Webstore Module allows for the on-line purchase of unlock codes that provide added software features and hardware functionality.

The Hardware **System 2 Upgrade** upgrades your **IXP220 Controller** from a Stand-alone Controller (with a locked Terminal Bus), to a System Controller. As a System Controller, you have support for up to 32 Anti-passback doors (dependent on your System type).

The Software unlock facility enables purchase of the following feature licenses (for use with System 3 and System 4 only):

- Web Tagholder Enrollment License
- Web Visitor Enrollment License
- Impro-Touch License
- Multi-site License
- Card Designer License
- Elevator Control License
- Input/Output Control License
- Notification License

IXP220 Utilities

Discovery Utility

This Utility allows the following actions:

- Detection of Controllers on the network.
- Detecting of IP Terminals (Door Controllers) on the network.
- Configuration of the network address settings.
- Configuration of the Controller's settings.
- Configuration of the Terminal's settings.

Universal Data Exporter Utility

The Universal Data Exporter Utility lets you extract transaction (including time and attendance) records from the IXP220 Database for use by third-party applications. The Exporter Utility makes use of user defined templates (created in Design Mode) that specify the data for extraction and the export format.

Using the Run Mode, you have the choice of exporting the records interactively or as scheduled (using Windows® Scheduler). Command line arguments specify the Mode and other parameters.

On installation of the IXP220 Software V1.80 (and upwards), two additional Utility shortcuts appear on the Programs Menu. These are **Universal Data Exporter (Designer)** (used for **Design Mode**) and **Universal Data Exporter** (used for **Run Mode**).

This Utility requires advanced knowledge of SQL.

Automatic Database Upgrade Utility

After completing the login action, the Automatic Database Upgrade Utility checks the IXP220 Database version. If the Utility confirms the IXP220 Database is older than that needed by the IXP220 Software, a Warning dialog tells you an upgrade is needed. If you do not upgrade the Database immediately, the IXP220 Software closes.

Database Conversion Utility

The Database Conversion Utility converts existing IXP120 or IXP200 Databases for use in IXP220. The Conversion Utility uses the same ImproX RS constraints as the IXP220 Software itself. This means the Utility checks for an ImproX RS and then checks the IXP220 System itself, confirming the number of allowed Tagholders and so on.

Note, the Utility does NOT move information such as Doors (Locations), Terminals, Controllers and so on. The Utility does move information such as Tagholder details, Tag information, Holidays, Messages, Reason Codes, Door Mode Patterns, Access Groups and Access Patterns. Therefore, at start-up, perform an Auto-ID of your Hardware and configure and link Doors (Locations) to Access Patterns.

Firmware Upgrade Utility

The Firmware Upgrade Utility lets you perform the following actions:

- Identify Firmware versions of connected Hardware.
- Selection and configuration of Communications Port.
- Ping the connected Hardware (provides confirmation that Hardware is connected and working).
- Perform in-field Firmware Upgrades to connected Hardware.

IBConsole Utility

IBConsole is a third-party database configuration and administration tool. You can use IBConsole to perform advanced configuration and administration tasks on the IXP220 Database.

Translate Utility

This Utility facilitates changing field names in the Database to another language. The Utility requires that you manually enter the replacement text.

Database Archive Utility

This Utility lets you archive transactions (Normal, Status and Alarms), placing the transactions in a separate archived Database. We recommend that you run the Archive Utility on a regular basis. Running the Utility regularly keeps your Database *below* the maximum recommended database size of **2 GB**. This action has the following major benefits:

- Manages the size of the Database, freeing up space on the PC.
- Keeps a cleaner, uncluttered Database.
- Keeps Database performance at optimum speed.

Database Pump Utility

The Database Pump Utility lets you flush out and correct a “muddled” or overloaded Database. When executed, the Pump takes ALL data and pumps this into a fresh Database.

IXP220 Network Specifications

The IXP220 Suite is designed to run over a network in Client-Server Mode. However, it *can* also run successfully on a single PC.

Architecture

Client-Server

Client-Server architecture consists of users' PC's (Clients) connected via a network to a central host (Server). In most situations, Client PC's are workstations that access files or databases, or applications running on one or more Servers.

In IXP220, the following are **Server** components:

- IXP220 Base Application
- Database

The rest of the applications are **Client** components.

Software Connection Relationships

Figure 1 shows the relationship between the IXP220 Database and IXP220 Client applications.

Socket connections enable communication between PC's. **Database connections** enable communication between PC's and the IXP220 Database. **Jaybird** is an interface component installed with IXP220, facilitating database interaction.

Network Hardware

An IXP220 compatible network requires the following hardware:

- **CAT5** or **CAT6 UTP** cabling
- **100 Mbps** or faster, **TCP/IP** enabled Network Interface Cards (NICs)

Routers

If routers or switches are used, they must conform to the following:

- **TCP/IP** protocol
- **100 Mbps** or faster

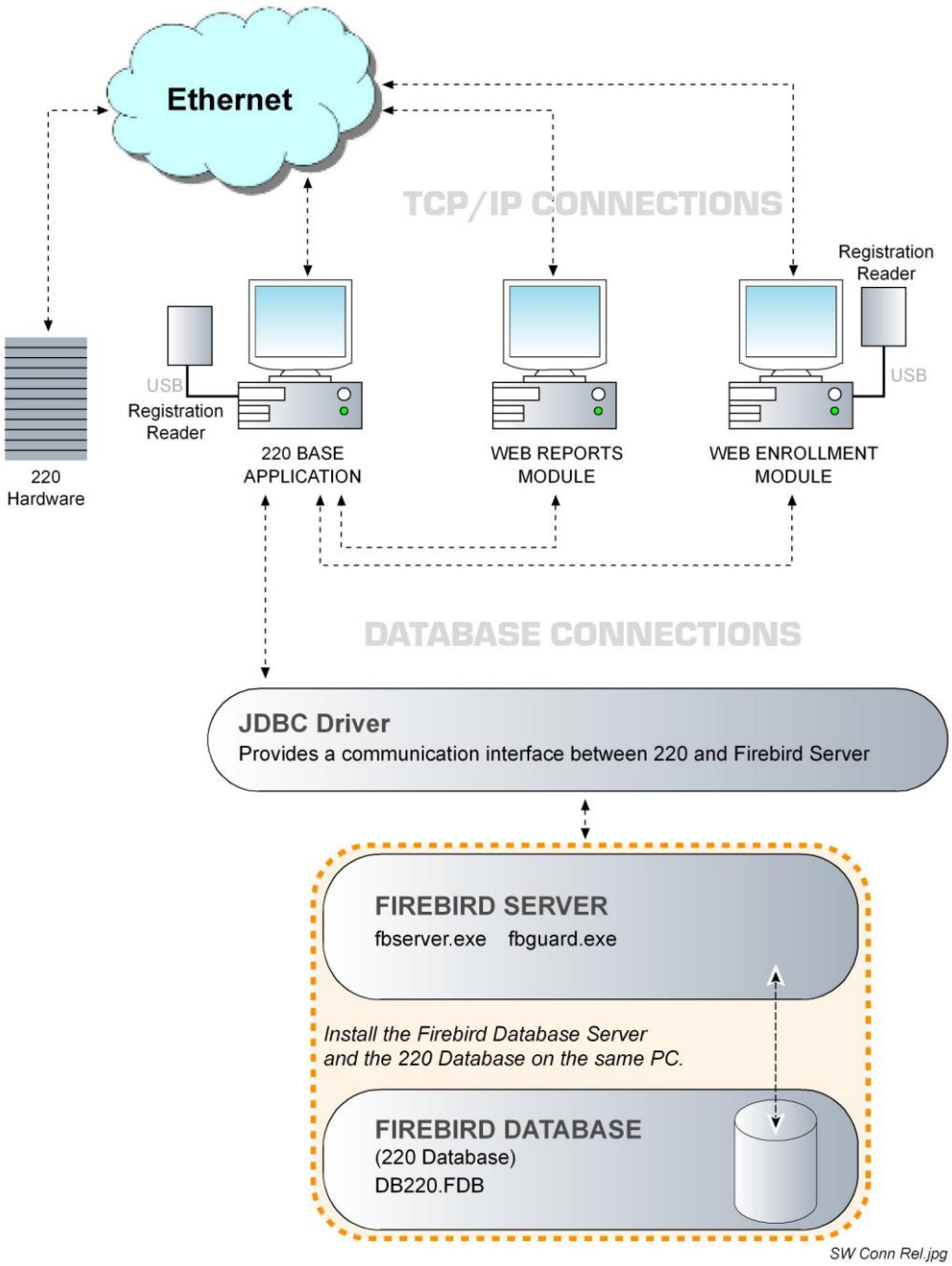

Figure 1 – Software Connection Relationships Diagram

IXP220 Modules in a Network Environment

The IXP220 Software is designed to run over a network in Client-Server architecture. However, all Modules can run on a stand-alone PC. The following components are important when running IXP220 over a LAN or WAN:

- IXP220 Database
- Firebird Database Server
- IXP220 Base Application

IXP220 Database

By default, IXP220 uses a **Firebird** Database. Firebird installs with the IXP220 Software, during the software installation process. The default location for the Database is as follows:

- C:\IXP220\Database\DB220.FDB

DB220.FDB *is the name of the database file.*

Firebird is an open-source product—it has no licensing fee. For more information refer to the following websites: http://www.opensource.org and http://www.firebirdsql.org/.

Firebird Server

Firebird Server is a Database Server program that facilitates connections between the **IXP220 Database** and the IXP220 Base Application.

Install Firebird Server on the same PC as the IXP220 Database.

IXP220 Base Application

The IXP220 Base Application functions primarily as a **Communication Server**. It performs the following functions:

- Retrieves transactions from IXP220 Controllers.
- Facilitates configuration of the IXP220 System.
- Monitors the IXP220 Database for changes.
- Communicates Database changes to the IXP220 Controllers.
- Runs the Web Server.

The **Web Enrollment** and **Web Reports Module** process and report information real-time. To do this, they use **TCP/IP** socket connections to connect to the Base Application.

Socket connections are also used to send messages to the Base Application.

General Network Requirements

The following requirements are essential for IXP220 to operate over a network:

- Network hardware must support the **TCP/IP** protocol.
- The network must support **100 Mbps** bandwidth or greater.

Running IXP220 across a LAN

Figure 2 illustrates the network configuration for running IXP220 Software across a Local Area Network (LAN).

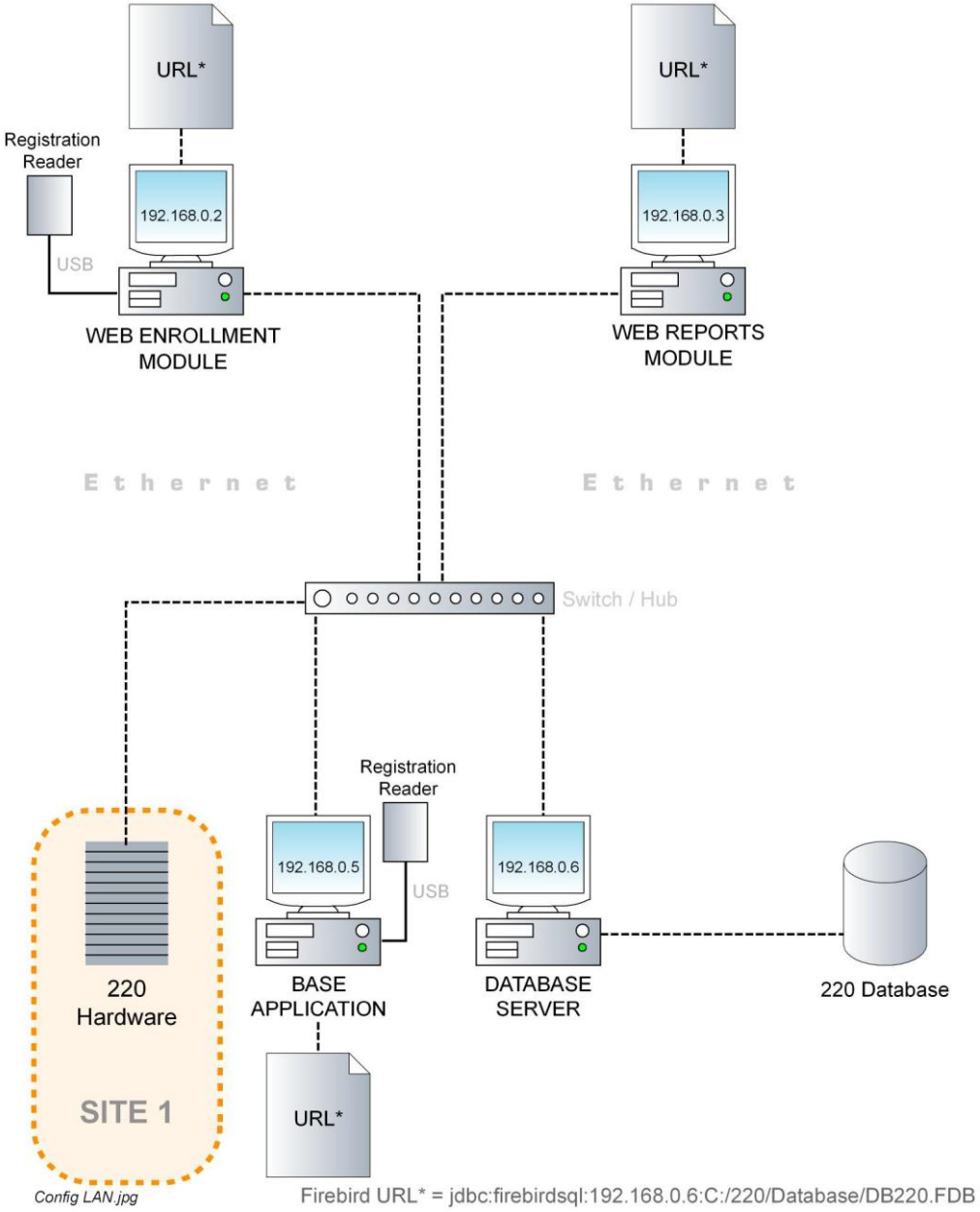

Figure 2 – IXP220 Configuration across a LAN

Running IXP220 across a WAN

Figure 3 illustrates the network configuration for running IXP220 Software across a Wide Area Network (WAN).

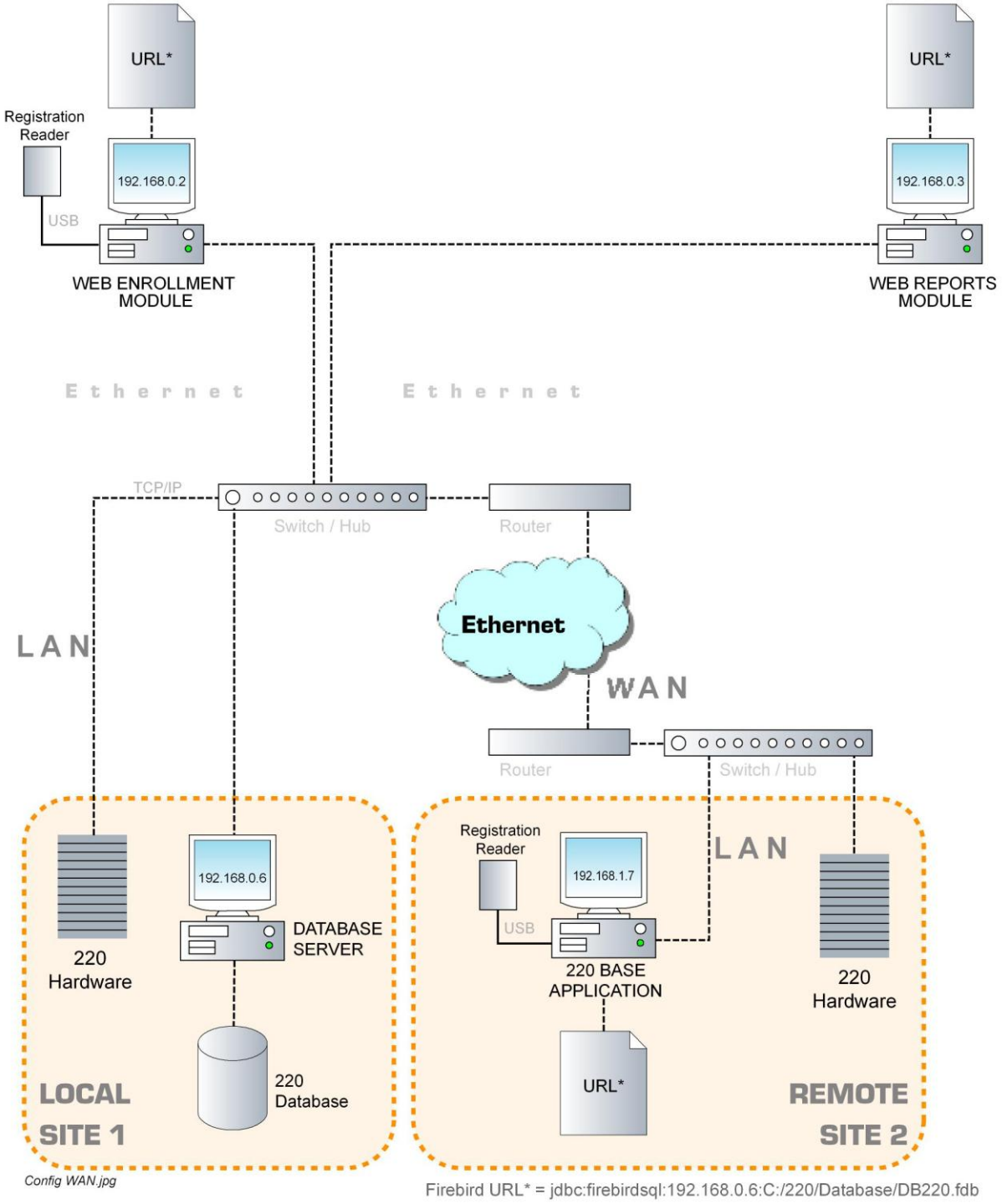

Figure 3 – IXP220 Configuration across a WAN

Communication across a WAN is generally slower than across a LAN. Therefore, carefully assess your WAN before implementing IXP220.

Minimum WAN Requirements

The Base Application and the Controllers (the Base Application communicates with) need a minimum throughput of 1 MBps. For example, a WAN capable of 2 MBps bandwidth, must assign at least 1 MBps for exclusive use by the Base Application and Controllers.

Properties Files

The IXP220 Base Application stores its connection settings in editable text files called **Properties Files**. These files contain URLs that specify the location of the Database Server. If the URL is incorrect, the application will not function.

Configuring IXP220 Modules for a Stand-alone (Single PC) System

This section provides the requirements for installing all IXP220 Modules, including the Database Server, on a single PC.

Connecting to the Database

The IXP220 Suite installs by default to **C:\IXP220**. The URL in the Base Application's **Properties File** points to the following default Database location:

- C:\IXP220\Database\DB220.FDB

If you move the Database to another location on the PC, you must change the URL in the Properties file to point to the new Database location.

For security reasons, we recommend that you do not share the Database folder.

The following extract shows the default format for the Database URL:

ixp220.database.Interbase.URL.0=C:/IXP220/Database/DB220.FDB

If you move the Database, you must update this URL to reflect the new location. For example, if you move the **DB220.FDB** file to a folder called **Site1** on drive **D**, you must change the URL to the following:

ixp220.database.Interbase.URL.0=D:/Site1/DB220.FDB

If you install other IXP220 Applications on the Database Server, the URLs in each Client Properties File must use a local path (for example "Localhost"), not a network path.

Configuring IXP220 Modules for a LAN (Firebird)

If you distribute IXP220 Modules across a LAN, at the **IXP220 Logon** dialog, edit the **Server Name** and **Database** URL accordingly. Modifying these fields automatically modifies the Properties file.

Configuring IXP220 Modules for a WAN

Running IXP220 across a WAN is similar to running IXP220 across a LAN. However, WANs generally have slower performance. IXP220 has options to minimize the resources required by a slower-than-usual architecture.

Advanced Base Application Settings

Figure 4 shows the Communications Configuration Dialog.

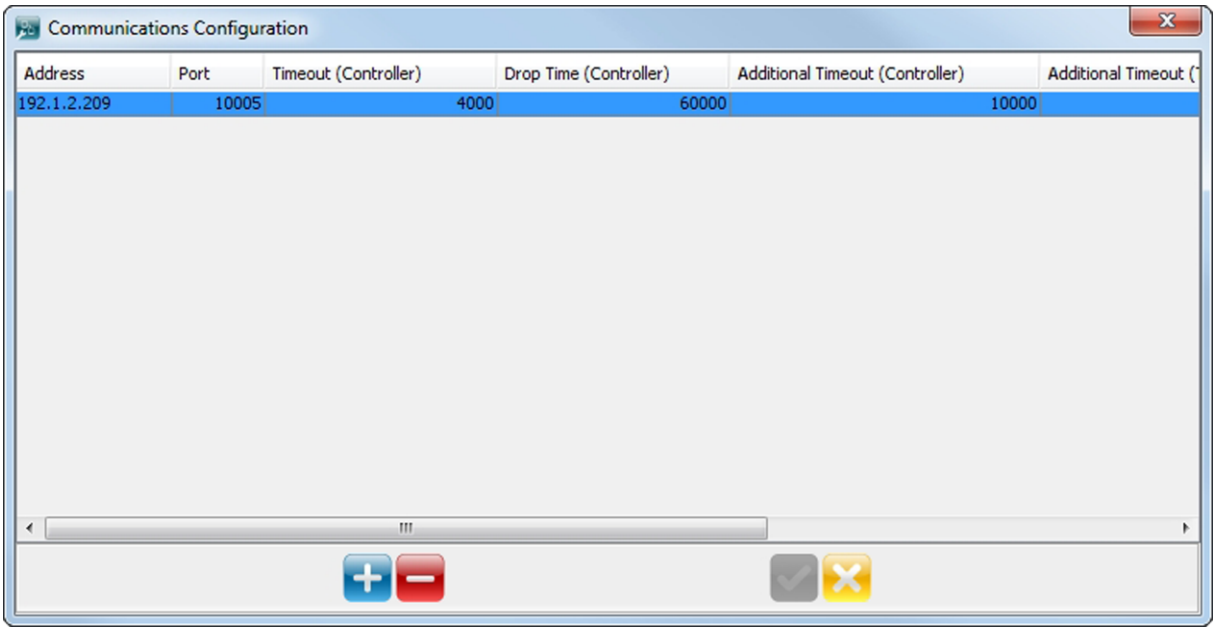

Figure 4 – Communications Configuration Dialog

Edit the following settings as required to compensate for the Base Application running across a WAN:

- **Timeout (Controller)**—is the duration for which the Base Application waits for a reply from a Controller. Increase this if using a WAN, a slow connection, Radio Modems, and so on. (For example, use a setting of 5 000 for EtherPADs). Also increase this setting if you receive many 'Controller Timeout' messages.
- **Drop Time (Controller)**—the duration for which the Controller will be dropped if it times out. This setting rarely requires changing.
- **Additional Timeout (Controller)**—an extra timeout value for increasing timeouts on the Controller bus. Increase this when fast polling Controllers across a WAN, a slow connection, Radio Modems, and so on. (For example, use a setting of 500). Ideally, disable fast polling for a WAN, a slow connection, Radio Modems, and so on.
- **Additional Timeout (Terminal)**—an extra timeout value for increasing timeouts on the Communication bus. Set this when Terminals are on a different network to the Controller. For example, when a controller connects to a Terminal across a WAN.
- **Inter Poll Delay**—the delay between successive polls. Use this to poll less often thus reducing network traffic over EtherPADs on a WAN (for example, use a setting of 2 000).
- **IC Port**—displays the inter-controller communications port number, that is the port used when controllers communicate with one another.

- **Respond Address**—displays the IP Address the IP Terminals use to communicate with the Controller.

Figure 3 on page 17 illustrates a possible IXP220 Configuration where a second site is connected via a WAN. In this type of scenario, it is important to determine how much bandwidth is available to the Base Application Server. If resources are limited, we recommend editing the advanced Base Application settings to further reduce the bandwidth that IXP220 requires to operate efficiently.

Using Routers Configuration

The following factors affect bandwidth when a router is used:

- Number of hardware devices configured in the Base Application.
- Number of Tagholders.
- Existing WAN load usage.
- Number of IXP220 client applications that access data via a router.

Router Configuration

WAN routers must enable *pass-through communication* on the port that the Database Server is using for connection. This is essential if the router has a built-in firewall.

Firebird Port

Firebird uses **Port 3050** by default. Therefore, ensure that WAN routers have **TCP/IP** enabled for network traffic sent to Port 3050.

Bandwidth Requirements

Every IXP220 installation will have different bandwidth requirements. For example, a Base Application that uploads 200 Tags to a single Controller can do so through a 64 k ISDN line. However, a Base Application that has to upload 5 000 Tags to five Controllers needs at least a 768 k dedicated ISDN line.

It is impossible to specify the exact requirement for a WAN. However, we recommend a *minimum* WAN connection bandwidth of **1 MBps**. For *optimal* performance across a WAN, we advise you to consider a connection with at least **2 MBps** of bandwidth.

Perform bandwidth-intense activities such as uploading Tag data to Controllers after-hours, thereby reducing network load during normal hours.

System Concepts

System Architecture Concepts

An IXP220 Access Control System comprises the following elements:

- Sites
- Controllers
- Doors (Locations)
- Zones

The IXP220 System Architecture is illustrated elsewhere in this Manual.

Sites

Each System consists of one or more **Sites**. Sites are independent of each other. Each Site can have only one Host. The Host is the **Base Application** Module for a particular Site.

Controllers

An IXP220 Site supports up to 64 **IXP220 Controllers**. Each Controller supports up to 64 **Terminals (Fixed Addresses)**.

Door (Location)

A Door (location) is a physical access control point. It comprises a group of **Terminals** servicing an access control point. A Door (location) supports up to two Terminals for the following functions.

- Door Entry
- Door Exit

Zones

A **Zone** is a group of Doors (Locations - access control points). Entry and exit to and from a Zone is achievable via its Doors (Locations) only. Generally, a Zone is a physically bounded area containing one or more Doors (Locations).

System Building Blocks

IXP220 Software Suite

The IXP220 Software Suite is designed to run on Microsoft Windows® XP (Professional), Vista (Business or Ultimate) and 7 (Professional, Enterprise or Ultimate). These limitations are important for the efficiency and reliability of the System.

Supervisory Elements—Host PC

Each Site requires a Host PC for control and supervision of the Site. Alternatively, multiple PC's can be used for the same function.

On a typical Site, the following functions are performed by the Host PC:

- **Database Server**—dedicated to the Site Database.
- **Base Application**—dedicated to processing communications between the Database Server and the Controllers. It also performs a polling function from the Server to the Controllers.
- **Client Workstation**—dedicated to supervisory aspects.

System Buses

The IXP220 System offers a choice of the following system busses:

- **TCP/IP Bus**—links the System Controller and Host PC to the LAN or WAN.
- **USB**—links the System Controller to the Host PC.
- **The Controller Bus**—this RS485 bus links the System Controller to the Host PC.
- **The Terminal Bus**—this RS485 bus connects each Controller to its Terminals. There is one Terminal Bus per Controller, with support for up to 64 Fixed Addresses.

Serial Peripheral Ports

Some hardware units have an RS232 Serial Peripheral Port. They can be connected to a single peripheral device.

Peripheral Hardware

IXP220 uses the following peripheral hardware devices to perform Tagholder registration and a Software unlocking function.

	Device Description
	The **ImproX (ISR) IXP220 Registration Interface** allows registration of 125 kHz and Mifare® (13.56 MHz) Tags into the IXP220 System using a third-party reader. The ImproX ISR connects direct to the PC and is powered by USB.
	The **ImproX (ISR) IXP220 USB Registration Reader** allows for Web-based enrollment or Base Application (in Systems IXP220-3 and IXP220-4) enrollment of **125 kHz Tags**. This Registration Reader does not support Impro Standard Tags or third-party Tags. This external Registration Reader connects direct to the PC via USB.

	Device Description
	The **ImproX (RS) Registration Interface** performs as follows: • Stores Hardware and Software license information. • Reads 125 kHz Tags when used with the ImproX (RRA) Registration Antenna Reader, (XRR901-1-0-GB-XX). • Reads MIFARE® 13.56 MHz Tags when used with the ImproX (RRM) Registration Remote Reader (XRM901-4-0-GB-XX). • Reads Wiegand Tags when used with the Wiegand Registration Reader (WRR900-1-0-GB-XX). The ImproX RS connects direct to the PC and is powered via USB.
	The **ImproX (MDE) Multi-discipline Enrollment Reader** allows for Web-based enrollment or Base Application (in Systems IXP220-3 and IXP220-4) enrollment of **125 kHz and 13.56 MHz frequency Tags**. This external Registration Reader connects direct to the PC via USB.
	The **ImproX B-SHO USB Fingerprint Enrollment Reader** and **ImproX B-SHO BioMini USB Fingerprint Enrollment Reader** are external enrollment readers that connect direct to the USB Port of the PC. These Enrollment Readers allow for registration of **fingerprints** for use by ImproX B-SHO Fingerprint Terminals. For more information on the use of these products with the IXP220 System, refer to Part 8 – Integration Modules.

Table 2 – Peripheral Hardware

Both the ImproX MDE and ImproX RS are supported on a single IXP220 system.

Software Installation Procedure

The IXP220 Software does NOT support Windows® 95, 98, 2000 or NT.

*Windows® Vista users must disable the **User Account Control** before installing the IXP220 Software. Disable the control as follows:*

1. *Select **Start**>**Control Panel**.*
2. *Select the **User Accounts** icon.*
3. *Select the **Turn User Account Control On or Off** option.*
4. *Deselect the **Use User Account Control (UAC) to Help Protect Your Computer** option.*
5. *Click the **OK** button.*
6. *Click the button.*

Log on to Windows® with Administrator privileges to install the IXP220 Software.

New IXP220 Installation

The IXP220 Software Suite is supplied on an installation **CD-ROM**. Before you install it, ensure you have read the following:

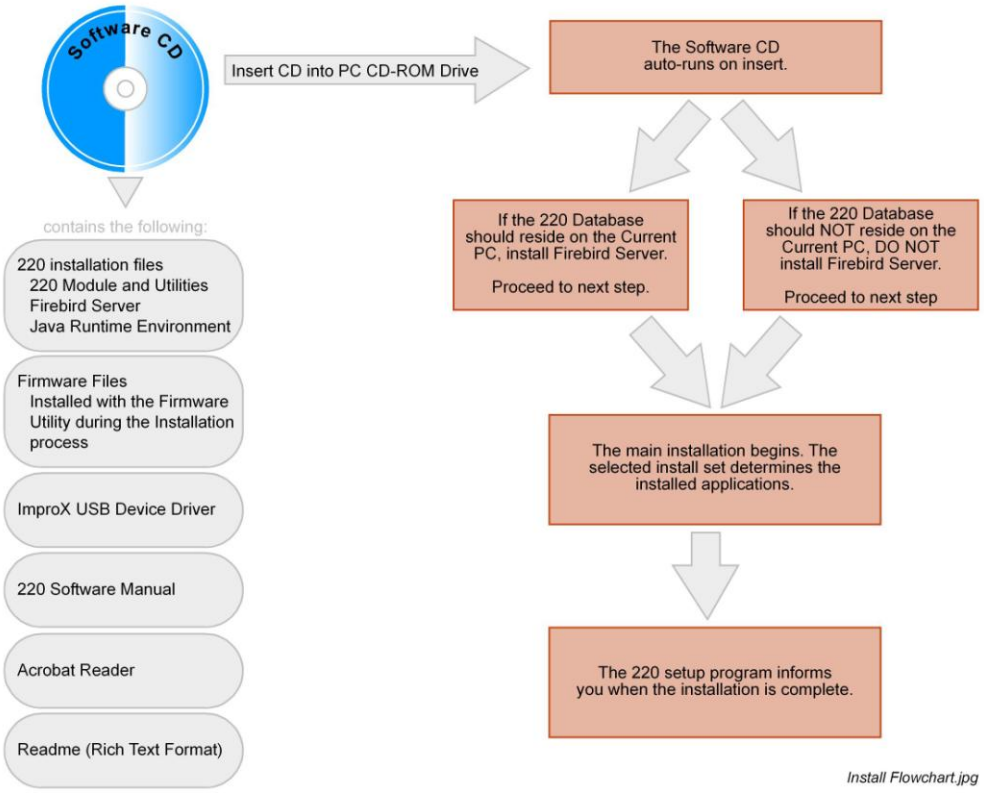

Figure 5 – IXP220 Software Installation Flowchart

PC Hardware Requirements

Refer to the section Minimum PC Specifications on page 5.

Installation Sequence

The IXP220 Installation CD uses an automated, interactive Installation **Wizard** to guide you through the installation process. The Wizard prompts you at various stages to select installation options. This makes it possible to customize the IXP220 Software Suite.

Install the IXP220 Software in the following sequence:

1. **Database Sever**—this is ESSENTIAL. Refer to the section, Installing the Database Server below.
2. **Applications**—Modules and Utilities.
3. **Database**—installed with the Base Application.
4. **USB Driver**—only required if your System makes use of USB Enrollment Readers or Controllers.

Installing the Database Server

A Database Server is required to host the IXP220 Database. If you install the IXP220 Software to a single PC, the Database Server installs automatically. However, if using more than one PC to host the IXP220 Software, install the Database Server manually.

Firebird automatically prompts to install, if a previous version is not detected.

Any PC on the network can host the Database Server. IXP220 uses **Firebird 2.1** as its Database Server. To install Firebird manually, proceed as follows:

Installing Firebird

1. Select a PC to host the Database Server.
2. Insert the IXP220 Installation CD in the PC's CD-ROM drive.
3. Browse to the **\database\firebird** directory on the IXP220 Installation CD.
4. Double-click **Firebird.exe**.
5. In the **Select Language Setup** dialog, from the drop-down menu, select your preferred language.
6. Click the **OK** button.

Firebird Installation Wizard

1. At the Welcome dialog, review and follow the on-screen instructions.
2. Click the **Next** button.
3. At the Licence Agreement dialog, select the **I Accept the Agreement** radio button.
4. Click the **Next** button.
5. Review the Information dialog, and then click the **Next** button.
6. In the Select Destination Location dialog, select the **Destination Directory**—we recommend that you use the default location of **C:\Program Files\Firebird\Firebird_2_1**.

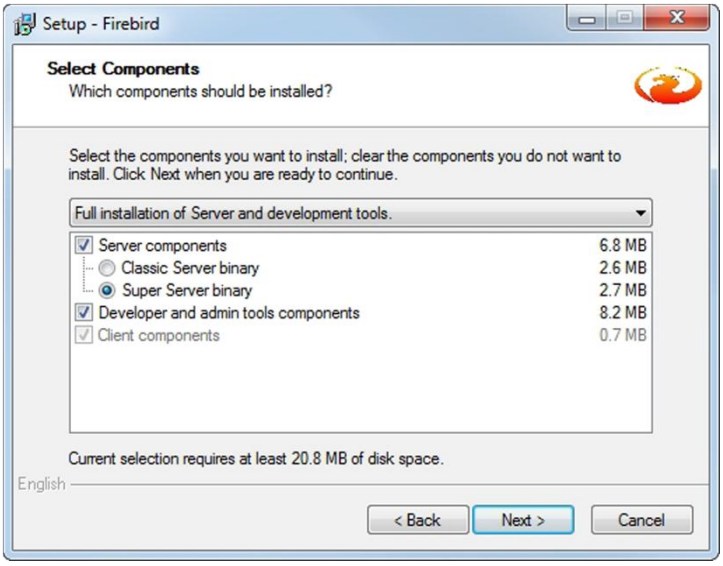

Figure 6 – Firebird Select Components

7. From the drop-down menu, select the **Full Installation of Super Server and Development Tools** option.
8. At the Select Start Menu Folder screen click **Next**.

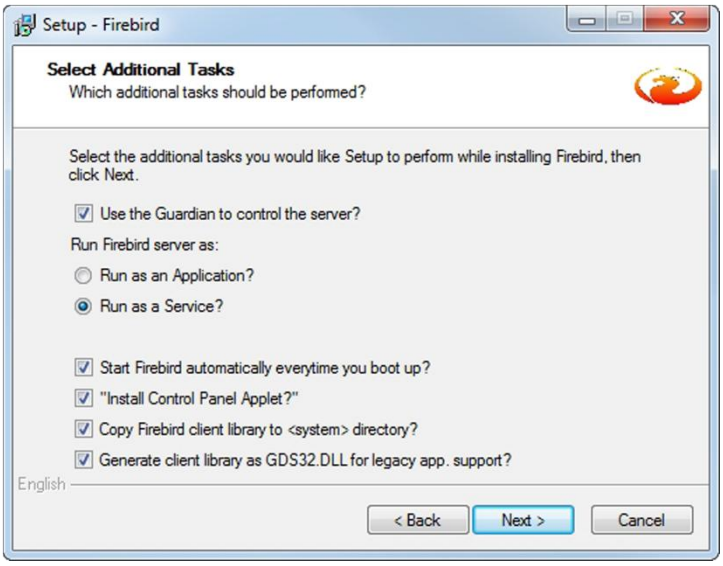

Figure 7 – Firebird Select Additional Tasks

9. On the Select Additional Tasks screen:
   – Select the **Use the Guardian to Control the Server?** option.

- Select the **Run as a Service?** option.
- Select the **Start Firebird Automatically Everytime You Boot Up?** option.
- Select the **"Install Control Panel Applet?"** option.
- Select the **Copy Firebird Client Library to <System> Directory?** option.
- Select the **Generate Client Library as GDS32.DLL for Legacy app. Support?** option.

10. Click the **Next** button.
11. Click the **Install** button.
12. Review the Information dialog and then click the **Next** button.
13. Click the **Finish** button.

IXP220 Installation Procedure

To install the IXP220 Software Suite on a single Host PC proceed as follows:

1. Insert the IXP220 Installation CD into the CD-ROM drive.
2. Select the **Install IXP220 Suite** option.

If the CD does not start up automatically, browse the CD in Windows® Explorer and double-click Setup.exe.

3. Select **English** as the language option.
4. Click the **OK** button.

If no Database Server is present, one is installed. Follow the onscreen instructions for this.

5. At the Introduction screen, click **Next**.
6. At the Licence Agreement screen, select the **I Accept the Terms of the Licence Agreement radio** button.
7. Click the **Next** button.
8. At the Choose Install Folder screen, click **Next**.

*If you change the installation directory file path, ensure that you enter **text only, NO spaces**.*

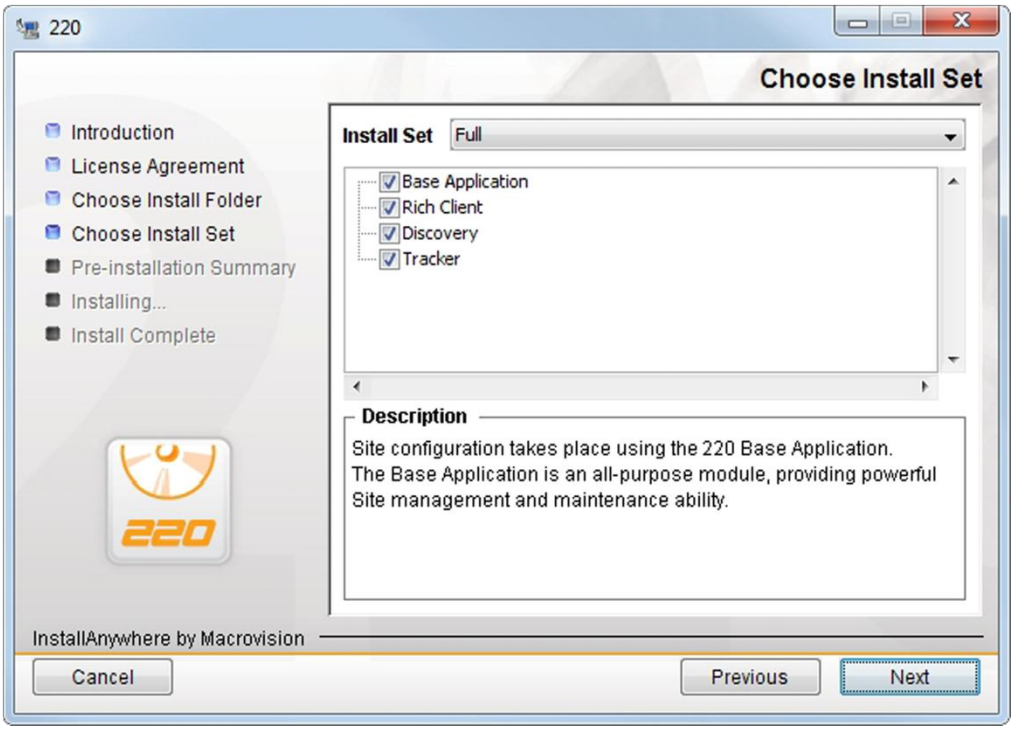

Figure 8 – Install Set Menu

9. At the **Choose Install Set** screen, from the **Install Set** drop-down list, make your preferred installation type selection.

An Install Set is a collection of pre-selected applications suitable for specific scenarios. Customize an Install Set option by selecting or de-selecting applications from the list.

10. Click the **Next** button.
11. Click the **Install** button.
12. At the Install Complete dialog, click the **Done** button.

By default Windows® XP (SP2 and SP3) installs a firewall. If you wish to keep this Firewall, ensure that you unblock the TCP Ports thereby allowing functionality of the IXP220 Software. Continue as follows:

1. *Select **Start**>**Control Panel**.*
2. *Select the **Windows Firewall** icon.*
3. *In the Windows Firewall Settings dialog, select the **Exceptions** tab.*
4. *Click on the **Add Port** button.*
5. ***Unblock the TCP Port** in the Add a Port dialog, by completing the **Name** (any name for example Impro) and **Port Number** (use **10005** for Ethernet Controllers) text boxes.*
6. *Select the **TCP** radio button.*
7. *Close the Add a Port dialog, by clicking the **OK** button.*
8. *At the Windows Firewall Settings dialog, again click on the **Add Port** button.*
9. ***Set the Ethernet Firebird Port** by completing the **Name** (any name, for example Firebird Service) and **Port Number** (use **3050** for Ethernet communication).*
10. *Select the **TCP** radio button.*
11. *Close the Add a Port dialog, by clicking the **OK** button.*
12. *Close the Windows Firewall Settings dialog, by clicking the **OK** button.*

*When using **separate PC's for the Base Application (Host PC) and Database (Server PC)** installation, continue as follows:*

1. *On the **Host PC**, install the IXP220 Software as listed under the section **IXP220 Installation Procedure**.*
2. *Stop the Firebird Server Software.*
3. *On the **Server PC**, install Firebird Server as listed under the section **Installing the Database Server**. Ensure that Firebird automatically runs as a service and that it has started.*
4. *Copy the Database file from the Database folder on the Host PC to the NEW Database folder on the Server PC.*
5. *Re-name the original Database file that remains on the Host PC to prevent you selecting it by mistake later.*
6. *Install the IB Console Utility on the Server PC, by copying the Utility from the **C:\IXP220\Tools** folder on the Host PC.*

Database Encoding

The default database uses **UNICODE-FSS** encoding.

Install the USB Driver for the USB Registration Reader Interface

The IXP220 Software uses a USB Registration Reader Interface to read Tags. Some Interface versions also provide an RS485 communication link to the Controllers.

The IXP220 Installation CD includes a USB driver for the USB Registration Reader Interface. You can find the USB driver in the following locations:

- The **USB_Device_Driver** directory on the CD.
- The **IXP220\USB_Device_Driver** folder on the Host PC.

To install the driver, proceed as follows:

*If there are pre-existing ImproX USB Device Drivers on the PC, delete them **before** installing the provided driver.*

*On some PC's, the **New Hardware Found** wizard displays every time you plug in a **USB Registration Reader Interface** with a new USB Serial Number (Fixed Address). If this happens, choose the option to automatically install the unit; the **New Hardware Found** wizard will not display again.*

1. Plug the **USB Registration Interface** into a USB port on the PC. The **Found New Hardware Wizard** displays.
2. Select the **Locate and Install Driver Software (Recommended)** option.
3. Select **I don't have the Disk. Show me Other Options**.
4. Select the **Browse My Computer for Driver Software (Advanced)** option.
5. Click the **Browse** button.
6. In the Browse for Folder dialog, select the **IXP220\USB_Device_Driver** folder.
7. Click the **OK** button.
8. Click the **Next** button.
9. At the Windows Security dialog, select the **Install this Driver Software Anyway** option.
10. Click the **Close** button.

You will notice that the Wizard pops up twice, installing two drivers; one for the **USB Registration Reader** and one for the **COM Port to USB Bridge**.

Upgrading an Existing Installation

1. **Backup the existing IXP220 Database** to a folder for safekeeping.
2. Copy the **Properties** files if running IXP220 on a LAN or WAN, to the folder for safekeeping.
3. Make a backup copy of the **Security2.fdb** file to the safekeeping folder. In a default installation you will find the **Security2.fdb** file at **C:\Program Files\Firebird\Firebird 2.1\security2.fdb**.
4. Uninstall the existing IXP220 Software.
5. Install the NEW IXP220 Software.
6. Ensure that the Database Server is **Firebird 2.1**. If not, uninstall the existing version and replace it with the newer version.
7. Move the backup **Security2.fdb** file to the new Firebird installation folder.
8. On installation of the Software, an empty Database automatically installs. Move the backup IXP220 Database file to the new Database folder, overwriting the empty Database file.
9. Upgrade the Controller and Terminal Firmware if necessary.
10. Upgrade the IXP220 Database if necessary.

*Ensure that you configure your IXP220 Controllers correctly **before** proceeding further with your IXP220 installation. Refer to Part 7 – Utilities for configuration information.*

Pre-configuration Procedure

It is critical that there are no communication problems prior to Software configuration. Otherwise, the System will not function.

*Ensure that the **Unit Location Chart** is correctly filled in when installing the Controllers.*

After installing all the 220 Software components, perform the **Pre-configuration Procedure**. This procedure ensures that the hardware communication infrastructure functions correctly.

RS485 Communications Infrastructure

1. Using the supplied USB Cable, connect the ImproX RS to the PC.
2. Using the IXP220 Controller's RS485 Controller Port, connect the IXP220 Controller to the ImproX RS.

USB Communications Infrastructure

1. Plug the **IXP220 Controller** into a USB port on the PC. The **Found New Hardware Wizard** displays.
2. Select the **Locate and Install Driver Software (Recommended)** option.
3. Select **I don't have the Disk. Show me Other Options**.
4. Select the **Browse My Computer for Driver Software (Advanced)** option.
5. Click the **Browse** button.
6. In the Browse for Folder dialog, select the **IXP220\USB_Device_Driver** folder.
7. Click the **OK** button.
8. Click the **Next** button.
9. At the Windows Security dialog, select the **Install this Driver Software Anyway** option.

Take note of the COM Port number displayed by the Driver Software Installation dialog.

10. Click the **Close** button.

TCP/IP Communications Infrastructure

*For **IXP220 Controllers and Terminals installed on the LAN** (that is the local Subnet of the Host PC), **make use of the Discovery Utility integrated with the IXP220 Base Application**. **For IXP220 Controllers and Terminals installed on a WAN** (that is the non-local Subnet of the Host PC), **make use of the stand-alone Discovery Utility** (local to the Controller or Terminal) **and export the configuration settings to the Host PC**. The Host PC runs the IXP220 Base Application.*

Ensure the PC running Discovery is on the SAME subnet as the IXP220 Controllers or Terminals for viewing.

View ALL Available IXP220 Controllers and Terminals on the Local Subnet

1. Using your chosen method, open the Discovery Utility:
   a. From the *IXP220 Base Application*, from the Menu Bar, select **Hardware**>**Unit Discovery**.
   b. Alternatively, start the *stand-alone Discovery Utility* from Windows® by going to **Start**>**All Programs**>**IXP220**>**Utils**>**Discovery Utility**.
2. On the Menu Bar, go to **Network**>**Search Local Subnet**.
3. If the Utility fails to find any Devices, at the **Device Not Found** dialog, click the **OK** button.
4. On the Menu Bar, go to **Network**>**Advanced Local Search**.

By selecting **Advanced Local Search**, you may select the correct **Network Interface** (only displayed where more than one exists) and enter the correct **Subnet Mask**. If the search returns Controller or Terminal details, the Utility (while running) retains the Network Interface and Subnet Mask information for further searches. You may however, use Advanced Local Search again during the session for further searches using different search criteria.

5. Select the relevant Network Interface, if more than one displays.
6. Click the **OK** button.
7. In the Input dialog, in the textbox, enter the **Subnet Mask** for your network.
8. Click the **OK** button. Wait for the Controllers and Terminals to display.

Sort the information displayed in either ascending or descending order by selecting the column header.

View a SPECIFIC Controller or Terminal

1. On the Menu Bar, go to **Network**>**Search IP**.
2. In the **Enter IP Address** dialog, enter the **IP Address** of the Controller or Terminal you're searching for.
3. Click on the button. Wait for the Controller or Terminal to display.

On display of Controllers and Terminals, the following icons appear: the icon represents unlinked Controllers. The icon represents Terminals and the icon represents Controllers with linked Terminals. On expanding the Controller tree, the icon displays, with the linked Terminals displaying below.

Secure Logon

1. In the **Device Password** dialog, enter your **password**. The default password is **masterkey**, for improved security we recommend that you change this password.
2. Click on the button.

Change the Secure Logon

1. From the Menu Bar, select **Configuration**>**Change Password**.
2. **Logon** if requested.

3. In the **Enter New Password** textbox enter a new password (not exceeding 16 characters) for the selected Controller or Terminal.
4. In the **Confirm New Password** textbox re-enter your chosen password.
5. Click on the button.

Grouping Controllers and Terminals

On display of Controllers and Terminals, the following icons appear: the icon represents unlinked System Controllers. The icon represents Terminals and the icon represents System Controllers with linked Terminals. On expanding the System Controller tree, the icon displays, with linked Terminals displaying below.

Creating the Group and Adding Controllers

There is no need to give a group name to a Controller if it has no IP Terminals.

1. Select the **Controller** and the **Terminal's** it should control.
2. On the Menu Bar, go to **Configuration**>**Add to Group**.

*Alternatively, right-click and select **Add to Group** from the pop-up menu.*

3. In the **Enter Group Name** dialog, enter a suitable group name for the selected Controllers.
4. Logon if requested (see page 32). A password is required for each Controller and Terminal being added to the Group.
5. Click the button.

Adding Terminals to Existing Controller Groups

1. Select the **Terminal(s)** to be added to the Group.
2. On the menu bar, go to **Configuration**>**Add to Group**.

*Alternatively, right-click and select **Add to Group** from the pop-up menu.*

3. In the **Select the Group Name** dialog, double-click on your chosen group name row.
4. Logon if requested (see page 32).
5. Click the button.

Communication Configuration – Case Local

Configure the Controller or Terminal's Static IP Address (Ethernet)

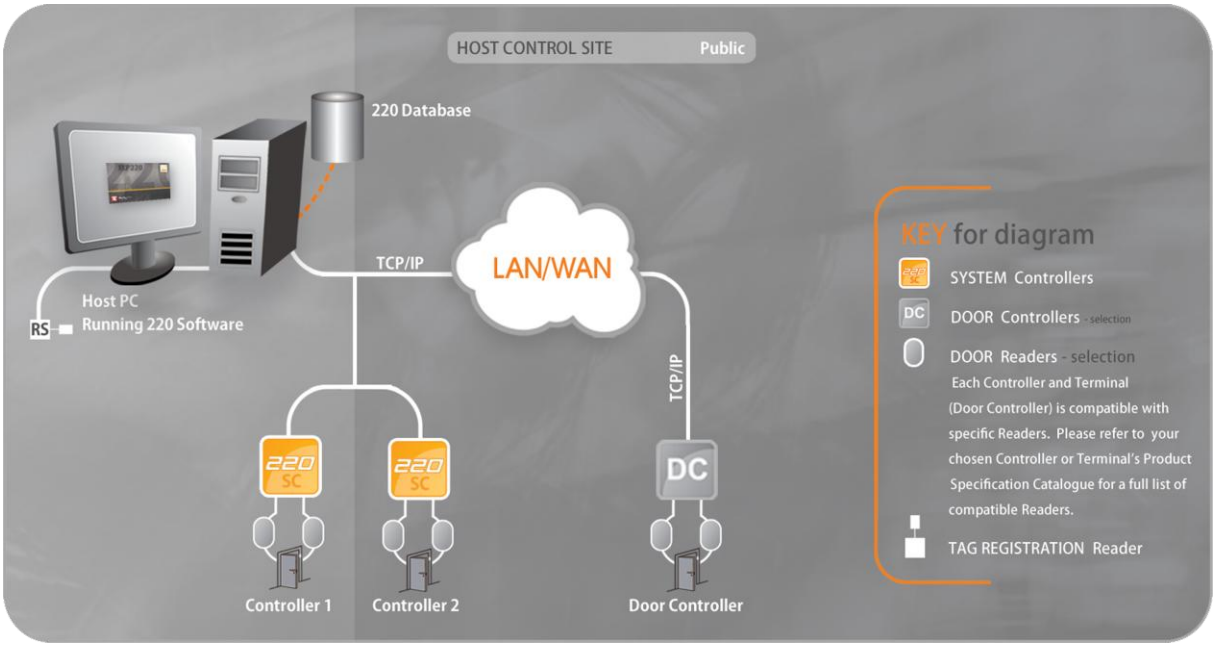

Figure 9 – Case Local—Configure the Controller or Terminal's Static IP Address (Ethernet)

If a DHCP server is present, IP Addresses are dynamically assigned initially. Obtain a suitable IP Address from your Network Administrator. A private static IP Address is essential for the Controller or Terminal because a DHCP Server may assign a new IP Address resulting in the Software losing communications.

If the Controller or Terminal is NOT on the DHCP Server, ensure the PC is on the same IP Range as that of the Controller or Terminal. If the PC's IP Range differs, you cannot change the Controller or Terminal's settings.

1. From the IXP220 Base Application, from the Menu Bar, select **Hardware**>**Unit Discovery**.
2. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
3. From the Menu Bar, select **Network**>**Configure IP**.
4. **Logon** if requested (see page 32).

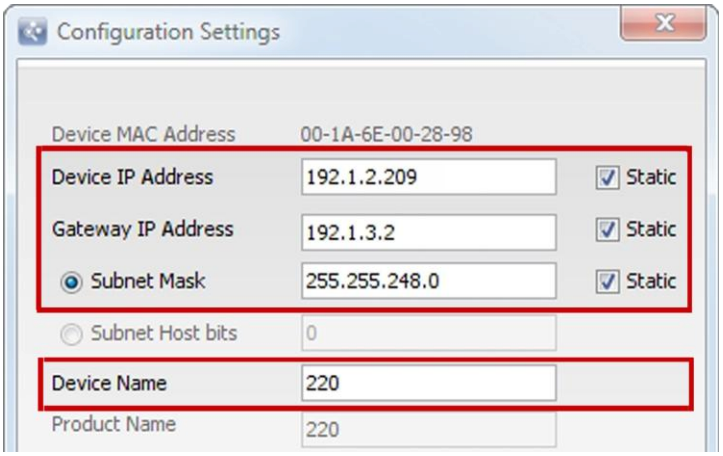

Figure 10 – Configuration Settings Dialog

By assigning an invalid IP Address, the Controller or Terminal may no longer communicate. Refer to the Hardware Installation Manual for information on restoring factory defaults.

5. In the Device IP Address textbox, enter a **Device IP Address**.
6. Tick the checkbox to set the IP Address to **Static**.
7. In the Gateway IP Address textbox, enter a **Gateway IP Address**.
8. Tick the checkbox to set the Gateway IP Address to **Static**.
9. Continue with *ONE* of the procedures (Subnet Mask *or* Subnet Host Bits) that follow:

   Subnet Mask
   a. Select the **Subnet Mask** radio button.
   b. In the textbox, alongside, enter the **Subnet's Address**.
   c. Tick the checkbox to set the Subnet Mask to **Static**.

   Subnet Host Bits
   a. Select the **Subnet Host Bits** radio button.
   b. Enter the number of bits in the textbox.

10. If necessary, amend the supplied **Device Name**. Use the same site prefix to name devices belonging to the same site. For example: "Site_1–Factory", "Site_1–Testing" and so on. Changes to the IP Configuration result in the Controller or Terminal rebooting on acceptance of the change. The Configuration Settings dialog remains open while allowing the Controller or Terminal to reboot. On closure of the dialog, the Utility again searches for the Controller or Terminal and if successful, displays the updated details.
11. Ensure the **Force Update** checkbox is **UNCHECKED**. If the Force Update checkbox remains unchecked, the Controller or Terminal changes the IP Address testing communication on the new Address. If successful, the update becomes final; if not, the Controller or Terminal reverts to its old settings.
12. Click the **Update** button.

After detection and configuration it's not necessary to assign a Logical Address, as the IXP220 Auto-ID process does this. It is not necessary to export the settings to a file.

Communication Configuration – Case Remote

Option 1: Configure the Controller or Terminal's Static IP Address (Ethernet)

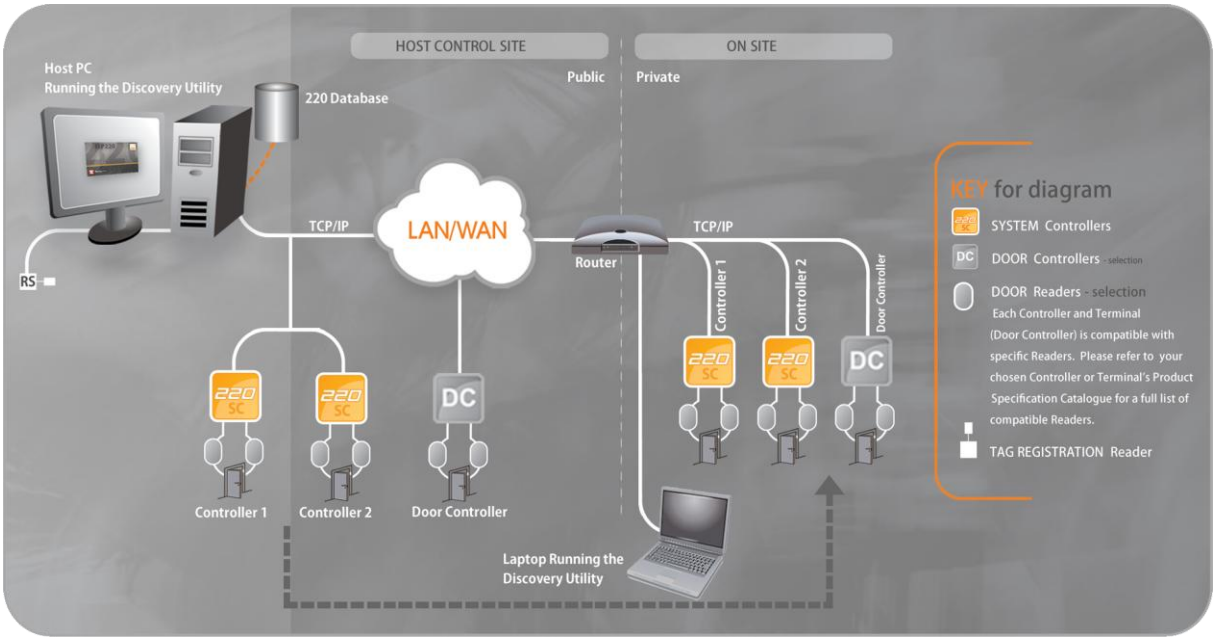

Figure 11 – Case Remote—Configure the Controller or Terminal's Static IP Address (Ethernet)

Use the stand-alone Discovery Utility on the same local Subnet as the IXP220 Controllers or Terminals for configuration. You may temporarily install and pre-configure the Controllers or Terminals on any convenient Subnet, local to the PC running the Discovery Utility. After configuration, move the Controllers or Terminals to the remote location. Alternatively, install the Discovery Utility on a PC on the remote Subnet. Export the settings to a file for manual entry into the IXP220 Base Application.

If a DHCP Server is present, IP Addresses are dynamically assigned initially. If the Controller or Terminal is NOT on the DHCP Server, ensure the PC is on the same IP Range as that of the Controller or Terminal. If the PC's IP Range differs, you cannot change the Controller or Terminal's settings. A ***public*** *static IP Address is essential for the Controller or Terminal because the Controller or Terminal is destined for a WAN.*

1. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**Discovery Utility**.
2. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
3. From the Menu Bar, select **Network**>**Configure IP**.
4. **Logon** if requested (see page 32).

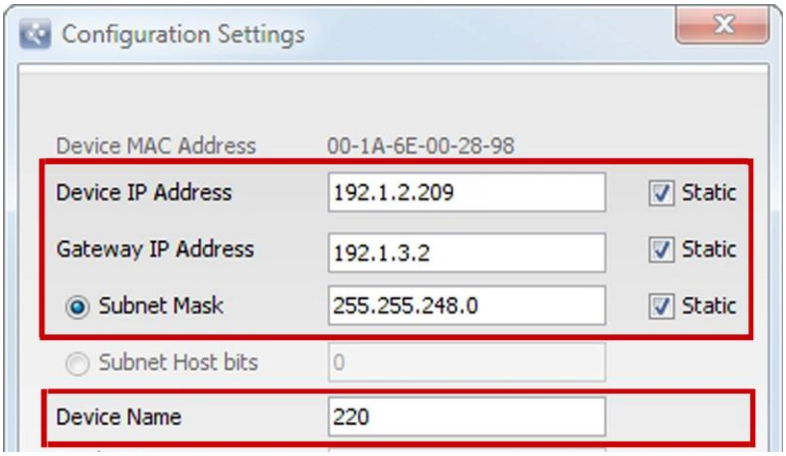

Figure 12 – Configuration Settings Dialog

By assigning an invalid IP Address, the Controller or Terminal may no longer communicate. Refer to the Hardware Installation Manual for information on restoring factory defaults.

5. In the Device IP Address textbox, enter a **Device IP Address**.
6. Tick the checkbox to set the IP Address to **Static**.
7. In the Gateway IP Address textbox, enter a **Gateway IP Address**.
8. Tick the checkbox to set the Gateway IP Address to **Static**.
9. Continue with *ONE* of the procedures (Subnet Mask *or* Subnet Host Bits) that follow:

   Subnet Mask
   a. Select the **Subnet Mask** radio button.
   b. In the textbox, alongside, enter the **Subnet's Address**.
   c. Tick the checkbox to set the Subnet Mask to **Static**.

   Subnet Host Bits
   a. Select the **Subnet Host Bits** radio button.
   b. Enter the number of bits in the textbox.

10. If necessary, amend the supplied **Device Name**. Use the same site prefix to name devices belonging to the same site. For example: "Site_1–Factory", "Site_1–Testing" and so on.

If the Force Update checkbox remains UNCHECKED, the Controller or Terminal changes the IP Address testing communication on the new Address. If successful, the update becomes final; if not, the Controller or Terminal reverts to its old settings.

Changes to the IP Configuration result in the Controller or Terminal rebooting on acceptance of the change. The Configuration Settings dialog remains open while allowing the Controller or Terminal to reboot. On closure of the dialog, the Utility again searches for the Controller or Terminal and if successful, displays the updated details.

11. Ensure the **Force Update** checkbox is **CHECKED** when assigning an Address on an external subnet. The Controller or Terminal changes the IP Address and reboots. If the Address points outside the Local Subnet, the Controller or Terminal is not found until it's physically moved to the new location.
12. Click the **Update** button.
13. From the Menu Bar, select **File**>**Export IP Config**.

14. In the Save dialog, click the **Save** button (by default this file is named **discovery.txt**, you may however change this file name).
15. Exit the Discovery Utility.
16. Send a copy of the exported Discovery file (**discovery.txt**) to the Host Location.
17. If locally pre-configured, move the Controller or Terminal to its remote location.

*After installing the Controller or Terminal in its new location, you can find it by going to **Network>Search IP**.*

Option 2: Configure the Controller or Terminal's Public Host Name (Ethernet)

Use this option where you install your IXP220 Controller or Terminal behind a Router with a public hostname resolved to an IP Address. In this scenario, the Router is setup (by your Network Administrator) to route data to the separate Controllers or Terminals via the port numbers uniquely associated with them. Detection of Controllers or Terminals using the Discovery Utility is only done locally, that is on the Local Subnet, behind the Router. To address the Controller or Terminal from the world beyond the Router, the local IP Address of the Controller or Terminal must change to the Router's public hostname.

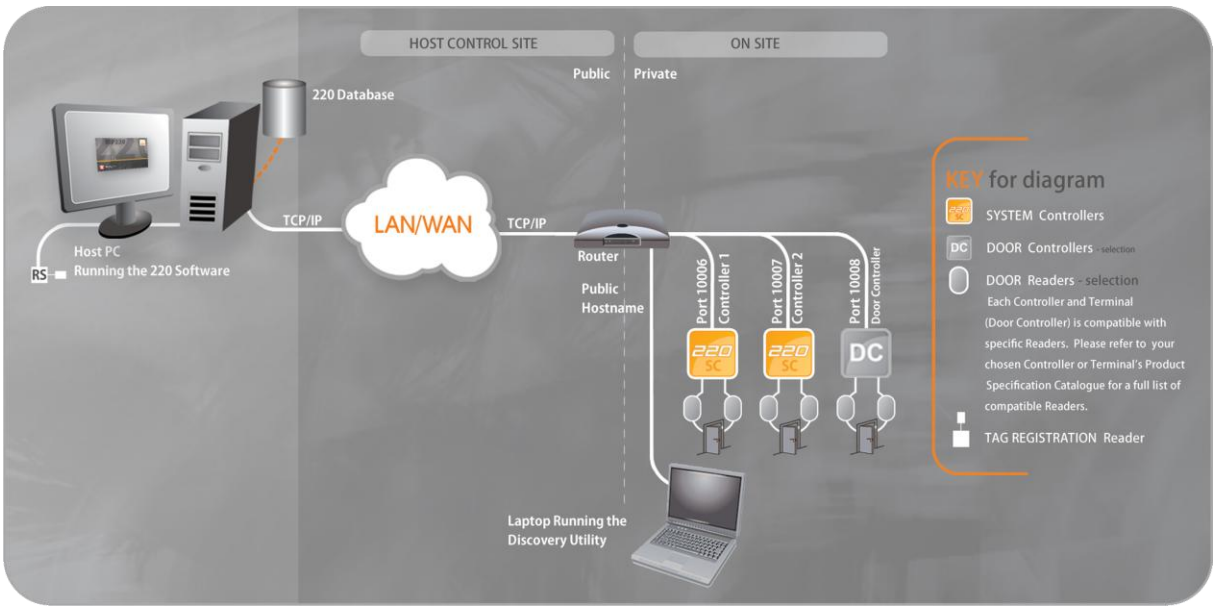

Figure 13 – Case Remote—Configure the Controller or Terminal's Public Host Name (Ethernet)

1. Select a UNIQUE Communication Port Number for the IXP220 Controller or Terminal.
2. Program the Router to direct all data destined for that port to the Controller or Terminal.
3. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**Discovery Utility**.
4. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
5. From the Menu Bar, select **Network**>**Configure IP**.
6. **Logon** if requested (see page 32).
7. Allow the DHCP assigned addresses to remain and set as static or obtain a static address from your network administrator.
8. If necessary, amend the supplied **Device Name**.

Change the Secure Logon and Clear the Controller or Terminal's memory as required.

9. Change the Communication Port Number to the unique port number set up on the Router.

10. From the Menu Bar, select **File**>**Export IP Config**.
11. In the Save dialog, click the **Save** button (by default this file is named **discovery.txt**, you may however change this file name according to your needs).
12. Exit the Discovery Utility.
13. Send a copy of the exported Discovery file (**discovery.txt**) to the Host Location.

In the IXP220 Software now add a new communication channel to your selected Site, either manually or by importing the file you exported earlier (**discovery.txt**). If the file is imported, the Port Number is correct and you need only change the IP Address to the Router's public Hostname. Auto-ID continues as normal. See Part 3 – General Configuration for full details on this procedure.

Option 3A: Configure the Controller's Mobile Settings (GPRS) for GPRS and SMS

This connection option is not supported where you have Controllers connected (by RS485) to the GPRS enabled Controller.

When configuring the GSM Module for GPRS and SMS ensure that you obtain a PUBLIC Access Point Name (APN) from your Mobile Service Provider.

When using a Hostname instead of an IP Address, ensure that you have access to a PC with an active Internet connection.

This option only applies to the IXP220 Controller fitted with a GSM Module.

Pre-configure the Controller with the Controller connected to the local LAN. After pre-configuration, remove the network connection from the Controller.

Pre-configuration, get the following from your Mobile Service Provider:

- Buy a **SIM Card** (you will need the **PIN** and **PUK** numbers for this SIM Card).
- Get a public **Access Point Name** (**APN**).
- Confirm details for the **SMS Service Centre**.
- Have the **Username** and **Password** for the Access Point Name (APN) available (only needed in some instances).

And from a Dynamic Domain Name Service Provider, get the following:

- Select one of the supported Providers, namely **changeip.org**, **dyndns.com** or **no-ip.com**.
- Register a **Hostname for your IXP220 Controller** with your chosen Provider.
- Register a **Username** and **Password** for your IXP220 Controller.
- Register a **Hostname for the PC hosting the IXP220 Software**, or use a public static IP Address.

Both Hostnames must resolve to a public IP Address, they cannot remain blank.

1. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**Discovery Utility**.
2. In the **Discovery Utility** window, select the Controller for configuration.

3. From the Menu Bar, select **Network**>**Configure Mobile Settings**.
4. **Logon** if requested (see page 32).

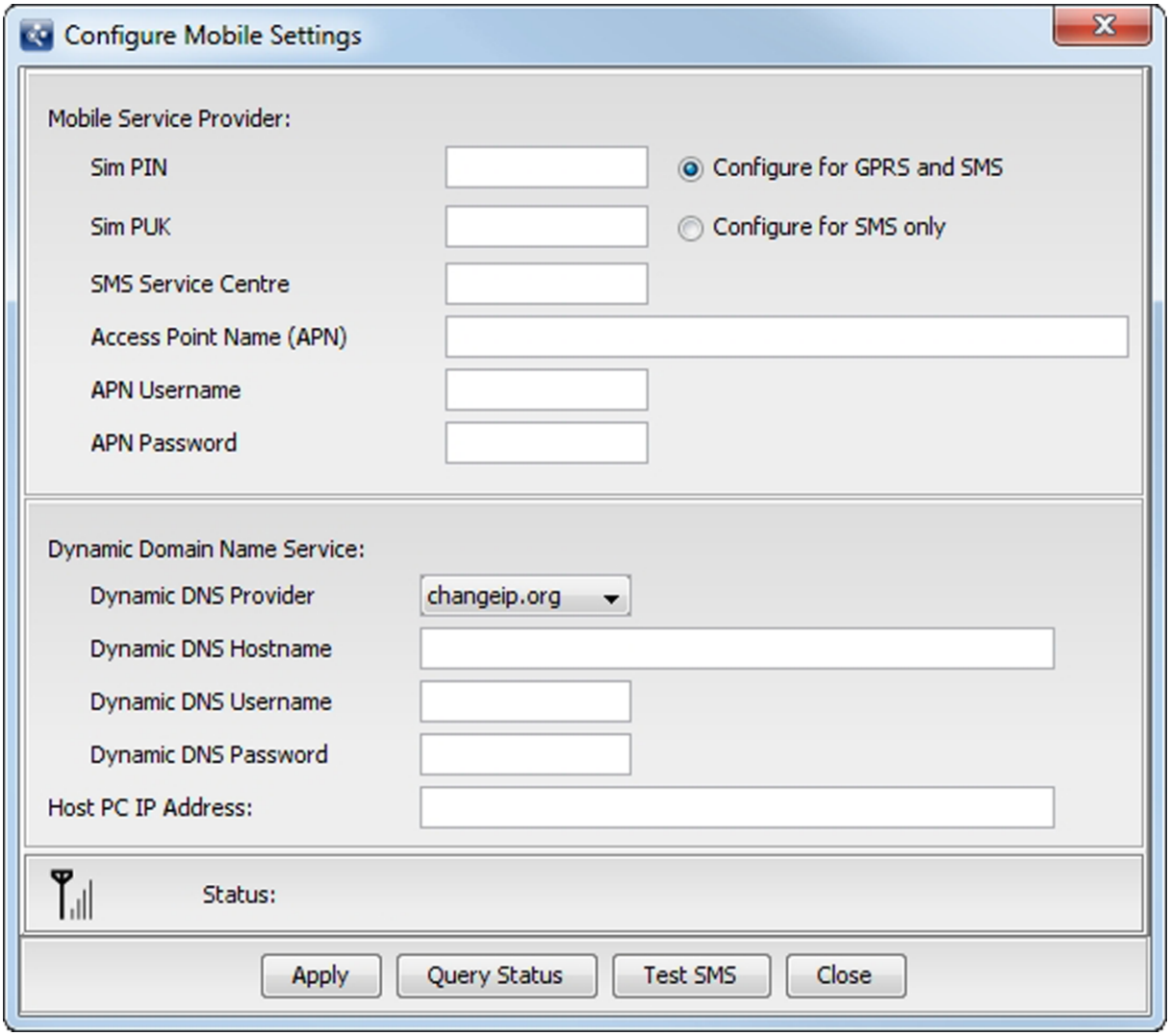

Figure 14 – Configure Mobile Settings Dialog

*The **Signal Strength** icon on the Status bar indicates the signal strength being experienced by the Controller's GSM Module. 5 Bars indicates maximum signal strength.*

5. Complete the fields under the header **Mobile Service Provider**:
   - **SIM PIN**—this is the Personal Identification Number (PIN), a numerical combination of up to 5 digits, supplied with your SIM Card. Wrong entry of the PIN (more than 3 times) locks the SIM Card.
   - **SIM PUK**—this is the PIN Unlock Key. This number offers protection of the device and SIM Card with the PIN. Entry of the wrong PUK (more than 10 times) permanently blocks the device, a new SIM Card is then required.
   - **SMS Service Centre**—the contact number for the repository that stores messages for delivery to the destination user when they are available. Stored on the SIM Card, this number may not come into sight until you activate your mobile settings. If you wish to use the service and the number does not finally appear, contact your service provider for assistance.

- **Access Point Name (APN)**—this is the name used to identify a public (free) GPRS bearer service in the GSM mobile network. The Access Point Name (APN) defines the type of service provided in the packet data connection.
- **APN Username**—possibly needed for the Access Point Name (APN).
- **APN Password**—possibly needed for the Access Point Name (APN).

6. Ensure the **Configure for GPRS and SMS** radio button is selected (default).
7. Under the header **Dynamic Domain Name Service**, From the **Dynamic DNS Provider** drop-down list, select one of the supported Providers.
8. In the **Dynamic DNS Hostname** textbox, enter the registered IXP220 Controller's Hostname.
9. In the **Dynamic DNS Username** textbox and **Dynamic DNS Password** textbox, enter the registered Username and Password respectively for your IXP220 Controller.
10. In the **Host PC IP Address** textbox, enter the public static IP Address.

When using a SIM Card with a single static IP Address, enter the public static IP Address of the Host PC, not the Hostname. Contact your Mobile Service Provider for more information on your SIM Card.

11. Click the **Apply** button.

The Discovery Utility captures the configuration information and forwards the information on to the Controller for activation. The Controller starts the process of establishing a GPRS connection. The Discovery Utility queries the Controller for status until the Utility gets a result. During the verification process there is an approximately *60-second time-out.*

The Discovery Utility decides on the success of the configuration. At the end of the verification process, the Status bar at the bottom of the Configure Mobile Settings dialog, displays the status of the configuration. Possible status messages include:

- **Listening**—this is the desired status message.
- **GSM Module Not Present**—indicates the GSM Module is removed or uninstalled.
- **GSM Module Present**—Controller is aware the GSM Module is connected; however the Controller is busy going through the connection process.
- **SIM PIN or PUK Error**—indicates you have captured the wrong PIN or PUK number.
- **GPRS Network Error**—indicates the GSM Module cannot connect to the Network.
- **APN Error**—indicates the wrong APN Name was captured. This message also appears however, where you have exceeded your data cap or you have no available airtime on your SIM Card.
- **DDNS Error**—indicates there is an error with the captured DDNS parameters.
- **Connected**—connected status only occurs if a Controller was already configured and currently connected by GPRS to the IXP220 Software while still connected by Ethernet.

*If the connection is not established, the Controller may begin the verification process again. In an instance where the verification process times out, click the **Query Status** button manually requesting the status.*

*If you do NOT get the status **Listening**, correct any errors and then press the **Apply** button again.*

On acceptance of the settings, the GPRS parameters are written to the **DiscoveryGSM.txt** file. The IXP220 Software automatically imports this file for permanent storage in the Database (in

case of Hardware replacement).

12. On achieving the Listening status, close the Configure Mobile Settings dialog.
13. Export the configuration file, from the Menu Bar, select **File**>**Export IP Config**.
14. Click the **Save** button.
15. Exit the Discovery Utility.
16. Send both **the DiscoveryGSM.txt** and **Discovery.txt** files to the Host PC (ensuring you place both files in the same destination folder) before beginning the Auto-ID process.
17. Disconnect the IXP220 Controller from the LAN.
18. Reboot the Controller.
19. Continue with the Auto-ID process (see Part 3 – General Configuration for more information on this process).

Option 3B: Configure the Controller's Mobile Settings (GPRS) for SMS Only

A public Access Point Name (APN) is NOT required for SMS only.

In instances where your Controller connects by Ethernet, but you still require SMS capability, continue as follows:

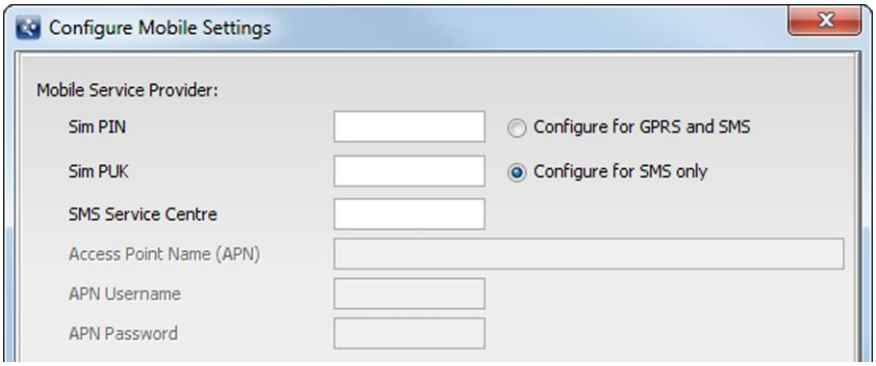

Figure 15 – Configure Mobile Settings Dialog

*The **Signal Strength** icon on the Status bar indicates the signal strength being experienced by the Controller's GSM Module. 5 Bars indicates maximum signal strength.*

1. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**Discovery Utility**.
2. In the **220 Discovery Utility** window, select the Controller for configuration.
3. From the Menu Bar, select **Network**>**Configure Mobile Settings**.
4. **Logon** if requested (see page 32).
5. Ensure the **Configure for SMS Only** radio button is selected.
6. Complete the fields under the header **Mobile Service Provider**:
   - **SIM PIN**
   - **SIM PUK**
   - **SMS Service Centre**
7. Click the **Apply** button.

*Your setup is complete and working correctly when you receive the Status message **SMS Configuration Completed**. We recommend that you test the connection by clicking the **Test SMS** button. Where called for by your country and or your service provider, precede the recipient's mobile number with the country code.*

USER NOTES

USER NOTES