InJoy Connect©

Configuration Guide

F/X Communications
Brolaeggerstraede 12
DK-4300 Holbaek
Denmark
http://www.fx.dk
support@fx.dk

November 1999

Contents

1 *Introduction*

This chapter discusses the following topics:

- Using This Manual
- InJoy Connect Software
- Product Highlights
- Preconfiguration Planning

1.1. Using This Manual

Welcome to the InJoy Connect (IC) PPP Server Installation and Reference Guide. This guide is intended for network administrators and others who will be installing, configuring and operating InJoy Connect.

The instructions in this guide assume that you are familiar with basic OS/2 operating system commands, TCP/IP, and that you know how to use a text editor to edit configuration files.

1.2. InJoy Connect Software

InJoy Connect (IC) is modular dial-in point-to-point (PPP) software, providing services for connecting your branch offices, mobile users and employees to headquarters.

IC provides reliable dial-in using standard telephone lines, leased lines or ISDN and high-end features makes IC one of the most powerful and secure software based Access Solutions available today.

IC is extremely easy to install (in less than a minute) and multiple demo configuration sets provide good examples and makes it easy to add your own setups.

IC incorporates comprehensive centralised management, modular design, RADIUS support, IPSec support, advanced packet filtering and extensive documentation.

IC provides enterprise scalability, allowing organisations to maintain concurrent user lists, easily add additional ports and even upgrade access topology on the fly.

IC offers a customisable Graphical User Interface with powerful control and monitoring capability for even remote servers.

Consultants who are tired of having to know a multitude of products for different sized clients can test IC on their home PC knowing it works exactly the same on large enterprise LANs.

1.3. Product Highlights

Modular Architecture
Launch any process -- anywhere -- and even in multiple incarnations, and on the fly.

Outstanding Scalability
Buy only the capacity you need -- Easily add new components. Disperse the dial-in topology and extend access on the fly.

Graphical User Interface
Real time control of (remote) Port Servers. Customisable user interface with powerful monitoring capability.

RADIUS Support
IC supports RADIUS for authentication, authorisation, and accounting (AAA), but can also function as its own centralised AAA server, even keeping the user-list in an exchangeable format!

Centralised Configuration
Central configuration in multiple database sets provides the flexibility to define logging, ports, modems, IP address pooling and users.

Filter Support
Filtering based on source and destination IP address, string-match, protocol or port. There is no packet that can't be matched.

IPSec Support
New levels of security through strong data encryption and IPSec based Virtual Private Networking (VPN).

1.4. Preconfiguration Planning

Before InJoy Connect can be used to connect wide area networks (WANs), you must install the software using the installation guide on a fully functional OS/2 computer with serial port support. This section will introduce the most common configuration options available and you should review this material before you configure your IC and if ask yourself the following questions:

- What configuration do you want to implement?
- What connection types do you want to offer (ISDN, Analogue Lines, leased lines)?
- Do you want to use multiport adapters?
- Do you want VPN support?
- Do you want packet filtering for Internet connections?
- Do you want to use SLIP, PPP or both?
- Do you want to use PAP/CHAP for authentication?
- Do you want local authentication or centralised authentication via RADIUS?
- Do you want RADIUS accounting for dial-in users?
- What level of diagnostic and trace information do you need?
- Do you need real-time monitoring of dial-in usage?
- Have you obtained the real-world IP network addresses or will you use internal (192.168.x.x) addresses for the dial-in users?
- Do you require IP, IPX (not supported by IC) or TCPBEUI?
- How do you want to configure dial-in users?

Many other decisions must be made during the configuration process, but the above should be considered before even entering the installation or configuration process.

2 *Installation*

This chapter provides instructions for installing the InJoy Connect software so you can choose how to configure your system.

This chapter discusses the following topics:

- System Requirements
- Installing the InJoy Connect Software
- RADIUS Servers
- Supported Dial-In Clients

2.1. System Requirements

In general, IC will run on any OS/2 version shipped later than ”Warp Connect 3.0 Connect”, including both Server and Workstation editions. The recommended installation for IC is OS/2 Warp 4 Workstation with the IBM 4.1 TCP/IP Stack. We cannot warrant error free operation on all the combinations of fixpacks that are available for OS/2, but no alarming results has been found in the beta testing phase.

For analogue access, you need serial ports (COM ports) and Hayes compatible modems. When serving multiple users, multi-port adapters are highly recommended and there are several vendors in the market that offers great support for OS/2. F/X Communications have tested IC with these multi-port adapters:

- DigiBoard Xi/8 - 8 ports
- DigiBoard PC/Xem - 16/32 ports

IC does not require long file name support, but notice that most RADIUS servers do.

The Minimum System requirements:

- Pentium 133Mhz CPU, with 32 MB of RAM.
- OS/2 version 3.0 Connect.
- TCP/IP Stack 4.0e.
- 20 MB of free harddisk space.
- Serial ports with modems.

  A modem for each port. High-speed modems are supported and recommended. IC was tested and developed for a variety of modem models.
  InJoy Connect servers require the following modem configuration:

  1. Auto-answer is on, making the modem answer any incoming call (usually ATS0=1).
  2. DCD (Data Carrier Detect) reflects true status of carrier (usually command &C1).
  3. When the DTR line turns off, the modem hangs up the phone line and switches to the command mode (usually command &D2).

- 16550 UART ports are suggested for best performance. IC will support older 16450 and 8250 UARTs, but at reduced speeds
- Free IP addresses (private or real world).

When using InJoy Connect as a dial-in server for strong encryption IPSec VPN clients, it is advised to use a powerful CPU (> 300Mhz). CPU encryption is per definition a CPU demanding task and greater key-length results in higher demands for CPU power.

2.2. Installing the InJoy Connect Software

InJoy Connect is extremely easy to install (in less than a minute) and multiple demo configuration sets provide good examples and makes it easy to add your own setups.

For successful installation, start with these steps:

1. Verify that the machine you have chosen to use as the IC server meets the requirements outlined in the "System Requirement" section.
2. If you have not already done so, we suggest that you read the README.1ST file before proceeding.

The InJoy Connect software ship as a zipped archive, ready for extraction into directly into a directory of choice.

Installation is simple, just follow these steps:

1. Unzip InJoy Connect.
2. Extract with Info-Zip's UNZIP.EXE (or PKUNZIP.EXE using the -d option) into the directory of choice.
3. Run install.cmd to have a Desktop Folder created.
4. That’s it!

If you are impatient and wants to get InJoy Connect running even before it’s configured, then switch to the ”/bin” sub-directory and start the ”run.cmd” command file.

2.3. RADIUS Servers

Remote Access Solutions often tie with RADIUS servers for offering services such as centralised authentication, authorisation and accounting (a.k.a AAA) of the dial-in users. IC has been tested to comply with the RADIUS protocol, and should work in combination with any RADIUS server, running on any Operating System.

Specifically, IC has been tested with the OS/2 port of the Livingston RADIUS 1.17 software, available at Hobbes (hobbes.nmsu.edu) and at the F/X Communications home page, at this URL: http://www.fx.dk/connect/radius.zip

This RADIUS server was tested by F/X Communications and has been found to operate well and reliable. It includes installation guidelines and it requires HPFS – at least for the %ETC% directory.

2.4. Supported Dial-In Clients

InJoy Connect has proven Dial-In capability and will probably work with ANY third party Internet dialer. Our official tests have proven successful connectivity with these Internet dialers:

MS Dial-up Networking Client (Win98)	MS RAS Client
InJoy Internet dialer for OS/2	DOIP for OS/2
SPRY's Internet In a Box	FTP's OnNet software

3 *How InJoy Connect Works*

Before configuring IC, lets step back for a while and study the design and the features offered by IC. This Chapter summarises IC operation and capabilities so you can choose how to configure your system.

This chapter discusses the following topics:

- InJoy Connect Design
- Scalability
- Graphical User Interface
- RADIUS Support
- Packet Filter Support
- IPSec VPN Support

3.1. InJoy Connect Design

IC is millennium proof 32-bit OS/2 software designed from the ground up to take advantage of multi-processing, multi-threading and TCP/IP based inter process communication.

3.1.1. InJoy Connect Executables

Every process is specialised to the task and modular design makes it simple to replace or add new modules without affecting the rest of the system. All atomic processes speak TCP/IP, providing good foundation for server distribution, centralised configuration and logging.

The InJoy Connect Software Modules at a glance:

 Graphical User Interface (“ICGUI.EXE”).
Provides control and monitoring capability.

 Port Server (“PORTSERV.EXE”).
Handles ports, modems and the actual Point-to-Point Protocol.

 Database Server (“DBSERV.EXE”).
Authentication, authorisation, accounting and RADIUS.

 Distributed Kernel (“FXKERNEL.EXE”).
Relay software for the other modules, forwards events.

3.1.2. Inter Process Communications

For Inter Process Communications (IPC), all modules set up a TCP/IP socket connection to the Distributed Kernel process. TCP/IP provides a very feasible implementation for IPC and even though there are faster approaches, TCP/IP compensates by means of added value:

- TCP/IP works over the intranet/Internet.
- TCP/IP allows for easy Deployment and Centralised Management
- TCP/IP can be traced via standard trace tools.
- TCP/IP is platform independent.

This architecture allows any module to specify the Network IP Address of the Distributed Kernel location, effectively enabling the possibility to distribute the entire system. Especially Port Servers benefit from the distributed approach, as it allows for direct dial-in in the regions where it is most feasible and cost effective.

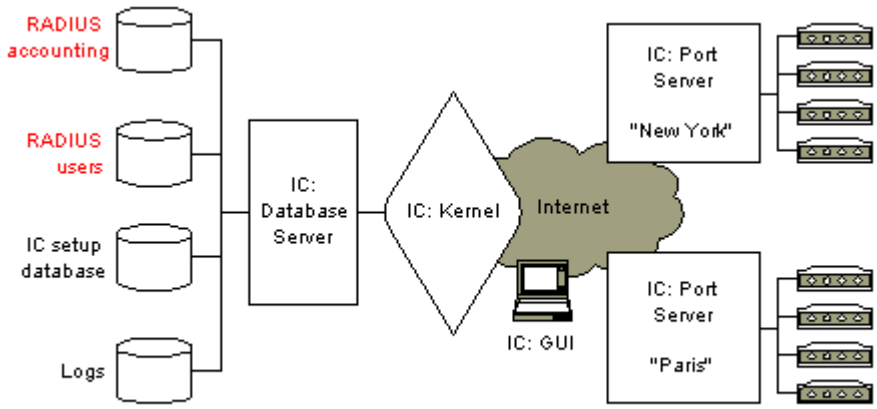
TCP port number 2697 is designated for protocol connection between the IC Kernel process and other IC processes. When the IC base system is installed centrally behind a corporate firewall and Port Servers/GUI's are running remotely, then the firewall must be opened for traffic on TCP port 2697

3.1.3. Modular Design

Definition: "Modular Architecture refers to the design of any system composed of separate components that can be connected together. The beauty of modular architecture is that you can replace or add any one module without affecting the rest of the system."

InJoy Connect is such modular software, also carefully designed to work by the principles of distributed computing. Distributed computing adds the possibility of connecting the modules over the Internet.
The tasks of IC are carried out by 4 specialised modules, each connecting to the Distributed Kernel via the TCP/IP protocol.

The context diagram below illustrates the modular architecture and the extremely open platform that prepares InJoy Connect to the many challenges of modern Access Servers.



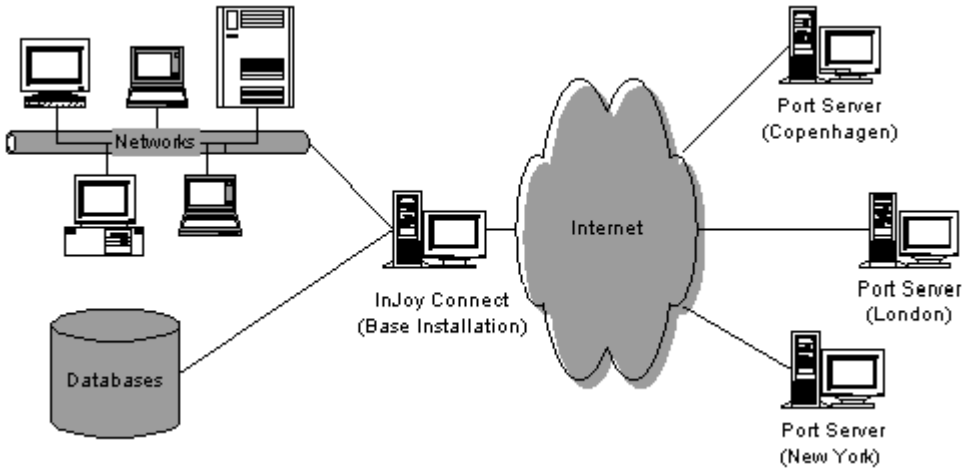
Example: With the distributed architecture you could install the user database on one PC, the actual Port Server on a different PC and from a third PC on the Internet you could monitor the whole system in action.

3.1.4. Centralised Management

Managing today's distributed systems, networks, applications and databases is a challenge for even the most skilled operators. Because critical information can come from different sources, and different locations, an operator must be able to access, recognise, and correlate events from different sources.

When properly managed, networks enhance productivity and lower costs by sharing resources throughout the organisation. With InJoy Connect, administrators get a unique possibility to effectively manage and maintain the server strategy from a centralised console. InJoy Connect can share resources, correlate information and even deploy settings to remote machines, making the task of operating complex systems easier. InJoy Connect takes advantage of the existing Internet to deliver a flexible, low cost solution.

The centralised management implemented by InJoy Connect eliminates the need to configure each Port Server separately, making the task of installing and managing a large number of ports much simpler and faster. Additionally, the centralised management allows for deploying Port Servers and modems in the region offering the most cost-effective dial up solution for your clients.



Central Authentication

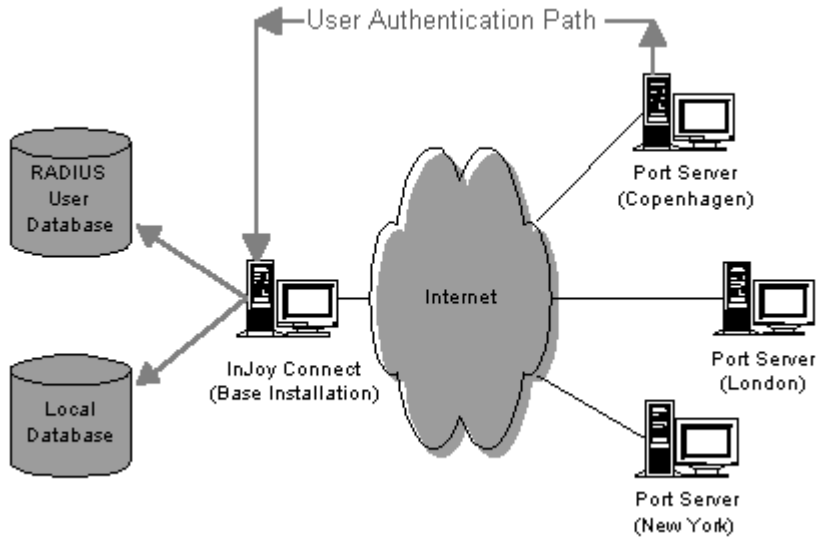
Since Remote Access Servers per definition offers a link to the outside world, they require careful attention to security, authorisation and accounting.

InJoy Connect supports the PPP protocols CHAP and PAP for remote user login and once the user has been identified, he or she needs to be authenticated.
IC offers two possible methods of authentication:

- Authentication via Local database
- Authentication via RADIUS server

The local user database is a simple ASCII file, using the same format as that defined by the RADIUS standard. The common format allows for concurrent user lists and the possibility to start small and grow big with easy porting of the user database to RADIUS.

The central authentication is easily achieved with the design incorporated by InJoy Connect. Illustrated below is the logical path of remote user authentication.



Central Accounting

Following a session with a remote user is the task of accounting. InJoy Connect supports RADIUS based accounting, with these key features:

Client/Server Model:
InJoy Connect operates as a client of the RADIUS accounting server. IC is responsible for passing user accounting information to a designated RADIUS accounting server.
The RADIUS accounting server can act as a proxy client to other kinds of accounting servers.

Network Security:
Transactions between InJoy Connect and a RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.

Extensible Protocol:
All transactions are comprised of variable length attributes. New attribute values can be added without disturbing existing implementations of the protocol.

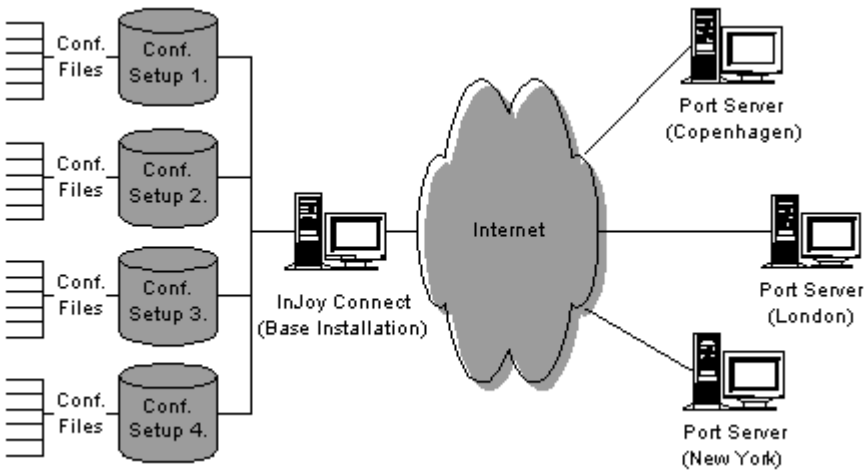
With InJoy Connect the following accounting attributes are supported:

- Authentication Method
- Session ID
- Session Duration
- Input Octets
- Output Octets
- Input Packets
- Output Packets
- Terminate Cause
- Class

Central Configuration

InJoy Connect offers configuration of a multitude of parameters. The parameters are divided into files and these files are divided into configuration sets.

The configuration is by means of simple ASCII files and the illustration below shows how files are organised into logical databases.



The groups of files are referred to as a “database file-set” or a ”database setup”. InJoy Connect supports multiple database setups, with each setup defining a profile to be used by one or more Port Servers. In other words, a Port Server must be associated with a setup before it can be activated.

Each file-set includes these files:

COMMENT.TXT	One line description of the configuration in this file set.
SERVER.CNF	Server options.
PORTS.CNF	Port definitions.
USERS.CNF	User Database.
IP-POOLS.CNF	IP pools for serving dynamic IP addresses.
AUTSTART.CNF	Autostarting of programs at certain events.
FILTERS.CNF	Packet filters.

Several sets of files can be stored on the InJoy Connect PC in individual directories, identified by the ".DB" file extension.

As an example, two sets of files have been defined below. The first setup defines a 4 port VPN setup and the other setup defines a 32 port setup. 1st setup is located in "bin/setup.db", while the other setup is located in "bin/setup2.db":

SETUP1.DB:

COMMENT.TXT	4 PORT RADIUS SETUP.
SERVER.CNF	Server options.
PORTS.CNF	Port definitions.
USERS.CNF	User Database.
IP-POOLS.CNF	IP pools for serving dynamic IP addresses.
AUTSTART.CNF	Autostarting of programs at certain events.
FILTERS.CNF	Packet filters.

SETUP2.DB:

COMMENT.TXT	32 PORT SETUP.
SERVER.CNF	Server options.
PORTS.CNF	Port definitions.
USERS.CNF	User Database.
IP-POOLS.CNF	IP pools for serving dynamic IP addresses.
AUTSTART.CNF	Autostarting of programs at certain events.
FILTERS.CNF	Packet filters.

3.1.5. Distributed Architecture

Made possible by the Distributed Architecture, it is possible to deploy geographically dispersed Port Serves and offer global access. For example, one Port Server can be installed remotely at a branch office, while another is installed locally at headquarters. Both Port Servers will automatically connect to the centrally running kernel process and receive the configuration of e.g. ports, IP-pools, filters, etc. In the other direction, the Port Servers will optionally send diagnostic information, user authentication requests and user accounting information.

New Port Servers can be installed on the fly, without affecting the rest of the system and Port Servers can even be remotely monitored and controlled via the PM GUI.

3.2. Scalability

Access solutions require a scaleable architecture to match toady's mission critical business solutions. With IC it is possible to seamlessly deploy Remote Access throughout your organisation, from the workgroup to the largest enterprise setting.

InJoy Connect Scalability Means:

- Deploy geographically dispersed Port Servers.
- Deploy extra IC Port Servers on the fly.
- Maintain multiple database sets.
- Monitor multiple Port Servers simultaneously.

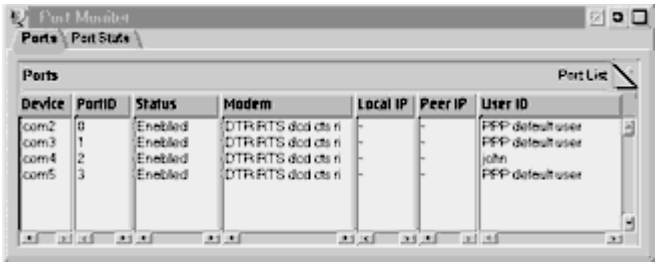
With the modular architecture of IC, it is possible to build a Global Access Network, using the power of OS/2. The Access Network is set up by installing the IC kernel and database module on a central OS/2 PC, and then installing remote IC Port Servers in every region that is to offer dial-in. The remote Port Servers connect to the IC kernel via the Internet, effectively making it possible to centrally control, monitor and configure the dispersed Access Network!

3.3. Graphical User Interface

InJoy Connect ships with powerful Graphical User Interface (GUI), providing real-time control of (remote) Port Servers. With a customisable user interface, the GUI ads powerful monitoring capability and with the modular architecture in mind, it is possible to skip the GUI and let InJoy Connect run unattended.

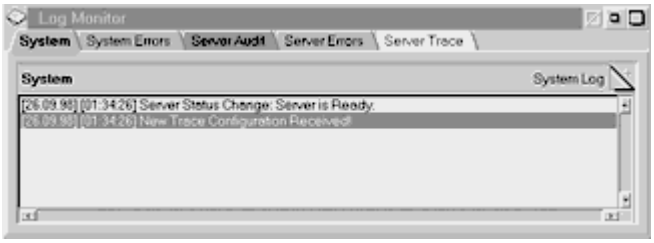
The GUI can run in multiple incarnations, each controlling one Port Server. The Port Server in question can then be controlled and monitored in detail. GUI control basically includes the selection of a Port Server, choosing a database, starting and stopping server.

Whereas monitoring is based on monitors, such as the Port Monitor:



The Port Monitor offers:

- List of ports/modems.
- Connected users.
- Enable, Disable ports.
- Port Statistics.



The Log Monitor is a customisable tool, allowing definition of multiple views presented in notebook style - each Log view denotes one tab in the notebook

The Log Monitor offers:

- Define new log-views.
- Centralised logging.
- Write to screen? File?
- Cached log file updates.

In addition to the above monitors, you will also find a Network Monitor in IC. This monitor provides a zoomable, landscape-like, visual overview of the Port Server - i.e. showing available and connected modems.

You can find other monitoring capabilities in InJoy Connect and also expect new ones implemented in the future versions.

The Graphical User Interface supports drag and drop of fonts and colors. Also, the GUI offers the possibility to save and delete saved window positions.

Remote configuration is currently only available via a telnet capable text editor.

3.4. RADIUS Support

3.4.1. Understanding RADIUS

Remote Authentication Dial-In User Service, or RADIUS (RFC-2138), is the standard for centralising the authentication, authorisation and accounting of remote access users.

Briefly, here's how RADIUS works: When a user dials in to a remote access device, that device communicates with the central RADIUS server to determine if the user is authorised to connect to the LAN. The RADIUS server performs the authentication and responds with a result -- either an ACCEPT or a REJECT. If the user is accepted, IC routes the user onto the network; if not, IC will terminate the user's connection. The RADIUS server also provides accounting services, if the remote access server can support this (IC does support RADIUS accounting).

With RADIUS, a network manager or ISP need only maintain a single, central database with which all remote user authentications happen. This greatly eases the management burden associated with administering large numbers of dial-in users.

3.4.2. From the RADIUS RFC

Managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorisation and accounting. This can be best achieved by managing a single "database" of users, which allows for authentication as well as configuration information detailing the type of service to deliver to the user (e.g. SLIP, PPP).

Network Administrators need to protect network services from unauthorised access by remote users. The strategy for verifying the identity of, granting access to, and tracking the actions of remote users is known as authentication, authorisation, and accounting (AAA). Remote Authentication Dial-In User Service (RADIUS) is commonly used to provide these solutions in today's inter networks

3.4.3. RADIUS Key Features

Please refer to the official RFC-2138 for more information.

Client/Server Model
An Access Server operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response, which is returned.

Network Security
Transactions between the client and the RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords sent between the RADIUS server and the client are encrypted.

Extensible Protocol
All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

3.5. Packet Filter Support

Packet filtering, by means of the F/X Packet Filter Plugin, allows TCP/IP packets to be selectively discarded as they flow through the plugin.

The Packet Filter Plugin allows ALL attributes in an IP-packet to be used as a filtering trigger to selectively discard packets when presented.

Supported Filter Criteria:

- Source / Destination IP numbers
- Protocol
- Service-port
- Bit Match
- Byte Pattern at Offset
- Byte Pattern Search
- Incoming traffic
- Outgoing Traffic

The Filter Plugin supports compound Boolean filters for complex filtering with great flexibility.

For easier navigation, filters are identified by linkable names and have a human readable comment attached.

3.6. IPSec VPN Support

3.6.1. Motivation for IPSec

Internet has shown its strength during the nineties. Most major corporations are now connected, and a large fraction of homes will be networked in the next few years. Though superior in its flexibility, the Internet has shown a major weakness; The lack of security.

Without encryption, anyone can read and tamper with the data sent over the network. Secrets can be stolen and mission critical data can be modified to cause irreparable harm.

Without proper authentication, anyone can easily lie about identity and it may be impossible to know whom you are doing business with or keep track if a crime has been committed.

Internet devices without protection are susceptible to external attacks. An attacker can get into internal data repositories, destroy information, install viruses, or just simply turn off or prohibit the services.

The obvious demand for a comprehensive security standard has finally been answered with the network vendor adoption of the IPSec standard.

3.6.2. Predominant VPN Standard

IPSec (Internet Protocol Security) is an Internet standard for interconnected, secure networking devices and the predominant technology in Virtual Private Networks (VPNs).

Below, 5 reasons why IPSec holds this position:

1. IPSEC has the widest industry support and is supported by e.g. Cisco, Microsoft, Network Associates, CheckPoint Software, Bay Networks, etc. This ensures interoperability and availability of secure solutions for all needs of corporate and private users.

2. IPSEC protects traffic transparently on IP packet level, as a completely transparent operation to the user. No changes in applications, no additional procedures or learning by the user required.

3. IPSEC is a native IP operation, not limited to e.g. operating system specific solutions. Unlike tunnelling protocols that can typically only be found in specific operating systems, IPSEC will be everywhere IP is. It will also be a mandatory part of the forthcoming IPv6 standard.

4. IPSEC has a wide variety of strong encryption standards and unlike previous solutions, IPSEC is a standard where security has been number one design criteria resulting in unbeatable security.

5. IPSEC includes a secure key management solution with digital certificate support. IPSEC guarantees the ease of management and use, even in large-scale networks and highly secure authentication of parties.

3.6.3. General IPSec Features

Data origin authentication
Verifies that the claimed sender originated each datagram.

Data integrity
Verifies that the contents of the datagram were not changed in transit, either deliberately or due to random errors.

Data confidentiality
Conceals the clear text of a message, typically by using encryption.

Replay protection
Assures that an attacker can not intercept a datagram and play it back at some later time without being detected.

Automated management of cryptographic keys and security associations
Assures that a company's VPN policy can be conveniently and accurately implemented throughout the extended network with little or no manual configuration. These functions make it possible for a VPNs size to be scaled to whatever size a business requires.

3.6.4. InJoy IPSec Plugin

The IPSec Plugin is developed by F/X Communications in line with the Internet Engineering Task Force (IETF) open framework for Internet Protocol Security (IPSec).

For a general description of the IPSec protocols, features, benefits and details, refer to the IPSec User's Guide.

Support of the IPSec technology extends the host product with capability of building VPNs and secure channels to other major vendors on the market. The IPSec technology is proven to be interoperable and since it is an international standard, it can negotiate safe communications between different organisations using different IPSec solutions.

A virtual private network (VPN) is an extension of an enterprise's private Intranet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel.

VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network.

Internet Service Providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers.

The InJoy IPSec Plugin can be used with the whole range of InJoy connectivity products:

- InJoy Dialer – For Point to Point dialing
- InJoy Connect – For Point to Point dial-in
- InJoy Firewall – LAN-2-LAN Internet Gateway and Firewall.

For more information about IPSec, please refer to the IPSec documentation included in your InJoy Connect archive.

4 Configuring Global Settings

Before configuring IC, you need to set up OS/2 so it will correctly handle traffic from your dial-in users. This Chapter summarises the IP stack modifications needed in order for InJoy Connect to work.

This chapter discusses the following topics:

- Setting the Default Route
- Network Routing Implications
- The Loop Back Interface
- IP numbers

4.1. Setting the Default Route

If you already know what a default route is and have it configured, then you can skip this section.

The default route (a.k.a. default gateway) is the address of the last resort router to which packets are sent when IC has no routing information for a packet. The default route is also the destination address IC selects when it cannot locate the destination of a packet on the local Ethernet segments.

The OS/2 PC running IC must have the default route set and typically, the default route is the route that directs the packets from the dial-in users to the next hop in the path to the Internet or to the Intranet server.

For further information on setting the default route, refer to routing section of the OS/2 TCP/IP documentation.

4.2. Network Routing Implications

The routing of dial-in users is done automatically on the InJoy Connect PC, but if you are running IC in network, then your network router needs to be updated as well. This can be done in two possible ways:

Automatically, using PROXY ARP
Automatic routing updates using PROXY ARP is turned off by default in InJoy Connect. The reason is that proxy ARP (a part of the TCP/IP stack) does not currently offer reliable support and stability for a 24x7 dial-up based server setup.

Statically, using normal routing
Modifying static routes is the recommend method for routing dial-in users on your network. Your network router must be configured to route:

- Packets destined for the dial-in clients.
- Packets coming from the dial-in clients.

Example:

Assume you plan to serve dial in users with IP addresses in the range of 10.2.2.x, then your network router should be updated with this route:

- Route add net 10.2.2.0 <IP address of IC> 1 netmask 255.255.255.0
  (Notice the syntax may vary – consult your router documentation for the exact syntax).

The route instructs the network router to send all traffic destined for the 10.2.2.x network, to the InJoy Connect PC – for further routing.

Your default route on the network router will make sure that packets coming from the dial-in users are routed to the next hop in the path to the destination.

Notice that IP addresses reserved for internal use (i.e. 192.168.x.x and 10.x.x.x) are not routable on the public Internet. Dial-in users using these reserved IP addresses must either be routed through a NAT (Network Address Translation) solution, a Proxy or another gateway solution to obtain Internet access.

4.3. The Loop Back Interface

The InJoy Connect software is multiprocess software that relies on the TCP/IP for interprocess communications.
The loop back interface (127.0.0.1) must be defined to successfully run IC. If you use the "run.cmd" command file to start IC, then the loop back interface will automatically be created for you.

4.4. IP Numbers

Two sets of IP addresses are available for use within the TCP/IP protocol:

1. Internic IP addresses routable on the Internet.
2. Private IP addresses reserved for use within companies.

As mentioned in the routing section, only true Internic assigned IP numbers can be routed through the public Internet. Private (a.k.a. Internal) IP addresses, defined in RFC-1918, are not intended to leave the intranet and if your dial-in clients are assigned internal IP addresses, then they must be routed through a NAT, Proxy or other gateway solution for Internet access.

Dial-in clients with private IP addresses can be routed on the company Internet, assuming company routing is configured to support the addresses assigned to the dial-in clients.

5 *Introduction to IC Configuration*

IC configuration is by means of flexible text files, organised into groups. Configuration of a Remote Access Server can be a challenging task, just as it is a challenging task for the RAS to deliver a flexible mechanism that can easily handle new options while preserving backwards compatibility.

This chapter discusses the following topics:

- Configuration Databases
- Configuration Files
- The Configuration File Format
- Compatibility

5.1. Configuration Databases

InJoy Connect organises configuration files into logical databases. One configuration database is a group of files organised into a directory with the extension ".DB". InJoy ships with a number of databases, demonstrating the various configuration options and these databases are found in within the InJoy Connect /bin directory as show below:

.\bin\default.db
.\bin\setup1.db
.\bin\setup2.db
.
.

Default, IC supports 10 configuration databases, whereof one of them is considered the default. The default database is named "default.db" and the Port Server at start-up automatically selects it, unless otherwise specified by command line options or by use of the IC GUI.

5.2. Configuration Files

All configuration options are stored in simple and well-organised text files, except for the diagnostic configuration file, which is created by the system and only editable through the GUI.

The text files:

COMMENT.TXT	One line description of the configuration in this file set.
SERVER.CNF	Server options.
PORTS.CNF	Port definitions.
USERS.CNF	User Database.
IP-POOLS.CNF	IP pools for serving dynamic IP addresses.
AUTSTART.CNF	Autostarting of programs at certain events.
FILTERS.CNF	Packet filters.

AND the only binary configuration file:

TRACE.DAT – per server trace logging and diagnostic configuration information.

5.2.1. Configuration Template Files

To avoid having to specify the same standard configuration parameters for each and every configured port, user, etc, InJoy Connect offers template files that specify the default values for

these records. In the actual records you then only need to specify the attributes that actually differs from the template definition.

The template files are named exactly the same as the ".cnf" configuration files listed above, but these files are located in the root of the IC "/bin" directory.

5.2.2. Configuration Descriptor Files

In the "/bin" directory of IC, you will also find files with the extension ".dct" extension. These files define the valid attribute and value pairs that make up the configuration. The ".dct" files should generally not be modified, but they can be used as a quick reference for discovering the possible values for a given configuration attribute.

5.3. The Configuration File Format

The configuration files are made up of attributes and values. Each attribute can have one value.

Example:

Com1	Port-Status = Port-Enabled,
	Port-Id = 1,
	Description = "Port 1",
	Default-User = "ppp_default",
	Speed = 115200,
	Authentication = CHAP-AND-PAP,

The above record is from the "bin/ports.cnf" file and it defines one port. The key is defined on the left and is in this case "com1". The attribute and value pairs are to the right and a comma must terminate each line.

Records begin in first position of a line. Attribute and value pairs are case-sensitive. Strings and IP addresses must be in quotes.

5.3.1. Compatibility

The local user database in IC is directly transferable to RADIUS servers, but if you have used special IC specific attributes, then the ".dct" file on the RADIUS server needs to be modified to support these options. If you plan to convert your local user database to RADIUS, then it is recommend consulting the RADIUS RFC standard prior to creating your user database. You will know that you are using InJoy Connect specific attributes in the user records when you see the attribute-names being prefixed with the word "InJoy".

The file format used by IC is generally the same as the file format used by popular RADIUS servers, but as RADIUS only includes a user database, then it is not feasible to directly convert the IC settings stored in other configuration files – e.g. "ports.cnf", "filters.cnf", etc.

6 *Configuring Per Server Settings*

InJoy Connect supports having individual software Port Servers connecting to the IC kernel to retrieve configuration details. This Chapter summarises the options that are configurable for each individual Port Server.

6.1. Per Server Attributes

Attribute	Possible Values	Description	Type
Status	Enabled Disabled	Specifies whether the database set is enabled or disabled.	Integer
Autostart-Control	Enabled Disabled	Specifies whether Autostarting is enabled or not.	Integer
Primary-DNS	Any IP address or “0.0.0.0”	The primary DNS Server dynamically assigned via PPP to the clients that support this. “0.0.0.0” allows the client to choose his own DNS server.	ipaddr
Secondary-DNS	IP address or “0.0.0.0”	Same as above, just the backup DNS server.	ipaddr
Proxy-ARP	Enabled Disabled	Use PROXY ARP to update network routing? Static routing is recommended over ARP. Refer to routing section.	integer
IPSec	Enabled Disabled	Enable IPSec? See IPSec documentation for further information on configuring IPSec once it is enabled.	integer
Accounting-Control	Enabled Disabled	Enable RADIUS accounting?	Integer
Radius-Control	Enabled Disabled	Enable RADIUS authentication?	integer
Radius-Timeout	Seconds	Time, in seconds that IC will wait for a RADIUS reply.	integer
Radius-Retries	Any number	The number of times IC will try to get a response from RADIUS.	Integer
Radius-Server	IP address	The IP address of the RADIUS server.	Ipaddr
Radius-Backup-Server	IP address	The IP address of the RADIUS backup server (if any). NOT SUPPORTED.	Ipaddr
Radius-Password	“string”	The password used to authenticate IC with the RADIUS server.	String
Radius-Service-Port	Any number	The UDP port number of the RADIUS user authentication service.	Integer
Radius-Acc-Service-Port	Any number	The UDP port number of the RADIUS accounting service.	Integer

Example:

TEMPLATE	Status = Enabled,
	Autostart-Control = Enabled,
	Primary-DNS = "0.0.0.0",
	Secondary-DNS = "0.0.0.0",
	Proxy-ARP = Disabled,

	IPSec = Disabled,
	Radius-Control = Disabled,
	Radius-Timeout = 5,
	Radius-Retries = 2,
	Radius-Server = "127.0.0.1",
	Radius-Backup-Server = "127.0.0.1",
	Radius-Password = "Pass",
	Radius-Service-Port = 1645,
	Radius-Acc-Service-Port = 1646,

The above example denotes the default settings, found in the “server.cnf” file, located in the “/bin” directory. The name “TEMPLATE” signifies that this record is one that contains default values. As there is only one of these records in each setup directory, the name you choose is of no importance to the system.

7 Configuring Ports

InJoy Connect supports up to 32 ports in each setup. The IC ports are configured in "ports.cnf" and this chapter summarises the options that are configurable for each port.

The key for port records is the device name, which you specify in the 1st position of a new line. See example.

7.1. Port Attributes

Attribute	Possible Values	Description	Type
Port-Status	Port-Off Port-Disabled Port-Enabled	Status of the Port. Port-Off means the port is completely turned off. Port-Disabled means the port will be disabled at start-up, but can be enabled from the GUI.	Integer
Port-Id	0..n	A unique ID identifies each port. This ID starts from 0.	Integer
Description	"string"	Free text description of the port record.	String
Default-User	"string"	The default user on this port, as long as a real user has not logged on.	String
Speed	9600 19200 38400 57600 115200 230400	The speed of the serial device.	Integer
Minimum-Speed	9600 19200 38400 57600 115200 230400	The minimum port speed of a modem connection. Not Supported.	Integer
Periodic-Init	Seconds	Number of seconds between periodic sending out of the modem init-string.	Integer
Init-String	"string"	Modem init-string.	String
Init-String1	"string"	Secondary modem-init string.	String
Disable-String	"string"	Disable modem string to get the modem out of auto-answer mode.	String
Disable-String1	"string"	Secondary modem-disable string.	String
DTR-Timer	Millisecs	Time to hold DTR low when IC disconnects the phone. On some modems, DTR must be lowered for as much as 2-4 seconds in order for the modem to drop the connection.	Integer
Flow-Control	NONE HDW-FLOW	The type of hardware flow control to use on the serial interface. HDW-FLOW (hardware CTS/RTS based flow control) is toady's standard.	Integer
Authentication	NONE PAP CHAP CHAP-AND-PAP	The type of authentication required for remote users. NONE means that a remote client can log-on without using any authentication protocol. PAP requires the use of PAP, CHAP requires the use of CHAP and CHAP-AND-PAP allows the PPP peer to choose a preferred authentication algorithm.	Integer
Authentication-	Enabled	Not supported.	Integer

Required	Disabled		
Aut-Restart-Timer	Millisecs	Milliseconds between sending out periodic PPP authentication packets. Less than 1500 is not recommended.	Integer
Aut-CHAP-Poll	Any Number	Not Supported.	Integer
LCP-Restart-Timer	Millisecs	Milliseconds between sending out periodic PPP negotiating packets. Less than 1500 is not recommended.	Integer
Max-Retries	Any Number	Max number of times the periodic PPP negotiating blocks will be sent out.	Integer
Prot-Comp	Enabled NONE	Use Protocol field compression.	Integer
Address-Comp	Enabled NONE	Use Address and Control field compression.	Integer
Autostart	Enabled Disabled	Is autostart enabled for the port?	Integer
Autostart-Connect	Key	Name of an autostart entry.	String
Autostart-Disconnect	Key	Same as above.	String
CAPI-EAZ	Any Number	Not Supported	integer

8 *Configuring Users*

This chapter describes how to configure InJoy Connect user tables to support dial-in connections. The user table settings define how each dial-in connection is made.

InJoy Connect supports authentication via a local database and via RADIUS accounting.

If you are using RADIUS, you must configure user attributes in the RADIUS user database rather than in the IC configuration database. The user file format used in IC is however compatible with that of the RADIUS server, so exchanging user databases between IC and RADIUS is possible.

For user databases with more than 100-200 users, it's recommended to use RADIUS with a binary indexed user database. Authentication via RADIUS is scalable, can be separated from the rest of the InJoy Connect system and the performance and user database can be tuned to fulfil just about any requirement.

8.1. User Attributes

Attribute	Possible Values	Description	Type
User-Name	"string"	The user-id that identifies the user. Must be specified in the 1st position on a line to form a new record.	String
Password	"string"	Clear text password for the user.	string
CHAP-Password	"string"	NOT a configuration attribute. Used internally to send a user's CHAP password to the RADIUS server.	string
Client-Id	IP Address	NOT a configuration attribute. The attribute is used internally for sending the IP address of the Port Server to the RADIUS server. This attribute is referred to as the "NAS-IP-Address" in the RADIUS standard.	ipaddr
Client-Port-Id	Any Number	NOT a configuration attribute. Used internally when authentication a user with RADIUS. The attribute will then contain the port number the user is logged into.	integer
User-Service	Login-User Framed-User Dialback-Login-User Dialback-Framed-User Outbound-User Shell-User	NOT a configuration attribute. Used internally when authentication a user with RADIUS. The attribute (a.k.a Service-Type) informs the RADIUS server of the service the user has requested. With IC, this field is always "Framed-User", as IC does not support text based logins or call back..	integer
Framed-Protocol	PPP SLIP	The protocol used by this user.	integer
Framed-IP-Address	IP Address Or 0.0.0.0	The IP address assigned to the dial-in user. If IP Pools are used, then this attribute will be overridden. Specify 0.0.0.0 to allow the dial-in client to pick his own IP address.	Ipaddr

Framed-IP-Netmask	IP Address	Specifies the subnet of the dial-in user. Typically the subnet mask for a point to point connection is set to “255.255.255.255”, indicating that the remote computer is single host (stand alone PC). If the subnet mask is e.g. set to “255.255.255.0”, then it indicates that the dial-in user has a network with 256 IP addresses behind the Internet Dialer (a class C subnet). Studying the subnet mask checking in TCP/IP literature is recommend.	ipaddr
Framed-Routing	None Broadcast Listen Broadcast-Listen	Specifies the routing to be performed for the dial-in user. This attribute is not relevant, nor used by InJoy Connect.	Integer
Filter-Id	“string”	Allows for attaching filters to individual users, by specifying one or more instances of this attribute. IC does not yet support filtering per user.	string
Framed-MTU	Any Number	The MTU is the Maximum Transmission Unit of the point to point connection. In other words, this attribute specifies the max size of packets transmitted to the dial-in user. 1500 is the recommend value. Refer to standard TCP/IP documentation for more guidelines about the MTU setting.	integer
Framed-Compression	None Van-Jacobsen-TCP-IP	This Attribute indicates a compression protocol to be used for the link. The Van-Jacobsen algorithm is popular and widely supported, but by toady’s standards almost rendered useless. It is recommend not using software compression, but instead turning on v42.bis compression in the modems. Refer to the Hayes AT command set for your modem.	integer
Login-Host	IP Address	NOT SUPPORTED. This Attribute indicates the system with which to connect the user, when the Login-Service Attribute is included.	Ipaddr
Login-Service	Telnet Rlogin TCP-Clear PortMaster	NOT SUPPORTED. Indicates the service, which should be used to connect the user to the login host.	integer
Login-TCP-Port	0..65535	NOT SUPPORTED. Indicates the TCP port with which the user is to be Connected, when the Login-Service Attribute is also present.	integer
Old-Password	“string”	NOT SUPPORTED. Often used proprietary.	String
Port-Message	“string”	This is the “success” message sometimes shown to the user after successfully	String

		authenticating with CHAP. Today, very few dialers support this and IC uses a hardcoded success message.	
Dialback-No	“string”	NOT SUPPORTED.	string
Dialback-Name	“string”	NOT SUPPORTED.	string
Expiration	A date	Proprietary RADIUS setting, sometimes used for expiration of users at a certain date. Not yet supported by InJoy Connect.	date
Framed-Route	“string”	Provides additional routing information for a user. One or more instances of this attribute can be specified in the configuration file. This attribute is hard to port from one access server to the other and as IC sets up its own routing, then this attribute is currently ignored.	string
Framed-IPX-Network	IP Address	InJoy Connect has no support of IPX.	ipaddr
Challenge-State	“string”	NOT SUPPORTED.	String
Class	Any Number	Available to be sent by the RADIUS server to the Port Server when a user is authenticated. The attribute is also valid if local authentication takes place and it will be used in the same way. The Port Server will send this attribute unmodified back to the RADIUS accounting server as part of the accounting information (if enabled). As the Port Server makes no interpretation, this attribute allows a RADIUS accounting server to easily link together user information with accounting information.	integer
Session-Timeout	Seconds	Max time for a dial-session. 0 disables in InJoy Connect.	integer
Idle-Timeout	Seconds	Max idle time before a dial-in session is disconnected. 0 disabled in InJoy Connect.	integer
Acct-Status-Type	A Number	RESERVED FOR ACCOUNTING. Not a configurable option.	integer
Acct-Delay-Time	A Number	RESERVED FOR ACCOUNTING. Not a configurable option.	integer
Acct-Session-Id	A Number	RESERVED FOR ACCOUNTING. Not a configurable option.	S ring
Acct-Authentic	A Number	RESERVED FOR ACCOUNTING. Not a configurable option.	integer
Acct-Session-Time	A Number	RESERVED FOR ACCOUNTING. Not a configurable option.	integer
Port-Limit	A Number	This Attribute sets the maximum number of ports to be provided to the user by the Port Server. Typically used when the same user-login is simultaneously used by a group of people or when Multi-Link PPP is in use.	Integer
InJoy-User-Note	“string”	Special IC option. Used as a comment field about the user for administrator convenience.	string
InJoy-Active	User-Passive User-Active	Special IC option allowing for easy updating of the user status. Either the user is active and is able to login, or the user is passive, hanging around in the configuration, but not able to login.	Integer
InJoy-Priority	1..100	Special IC option. Allows you to easily assign	integer

		idle priority to some users and critical priority for others. The default priority for a user is the OS/2 default, which evaluates to a priority value of approximately 60.	
InJoy-IP-Pool	“string”	The name of an InJoy IP Pool. See section about IP Pools.	string
InJoy-Autostart	Enabled Disabled	Specifies whether autostarting of programs is active for this user.	integer
InJoy-Autostart-Logon	“string”	Name of an autostart record to be executed when user has successfully logged on. The program will be executed the instant the Port Server gets the user-record, before PPP negotiation takes place.	String
InJoy-Autostart-Logoff	string”	Name of an autostart record to be executed when user has logged off. The program will be executed when the connection is dropped, but before the port is freed for new users.	string
InJoy-Autostart-Online	“string”	Name of an autostart record to be executed when user has logged on and the IP layer is up.	String

8.2. User Example

joe	Password = "test",
	User-Service = Framed-User,
	Framed-Protocol = PPP,
	Login-Host = 10.10.10.1,
	Framed-IP-Address = 10.10.10.10,
	Framed-Compression = Van-Jacobsen-TCP-IP

The above example illustrates a user record for the user “joe”, using the password “test”.

The Login-Host attribute value holds the IP address assigned to the local point to point interface on the Port Server. This IP address is of little interest and could basically be anything. The Framed-IP-Address is the IP Address assigned to the Peer – the dial-in client.

Refer to the sample user databases in your InJoy Connect archive for more examples and comments.

9 *Configuring IP Pools*

With the limited IP addresses available today, IP Pools is the preferred method for sharing a small set of IP addresses among a large group of people. The concept of IP Pools is based on each user being assigned a dynamic IP address, only active for the duration of one session. At the end of the session the IP number is freed for use by other users.

The attributes that make up the IP Pools are described in the table below:

9.1. IP Pool Attributes

Attribute	Possible Values	Description	Type
Pool-Name	“string”	The name of the IP Pool. This attribute must begin in the left position on the line and it denotes the key for the record.	String
Pool-Status	Enabled Disabled	Specifies whether the IP Pool is enabled for use or disabled.	Integer
Start-Address	IP Address	The first IP address available to dial-in clients.	Ipaddr
Range	1..256	The number of IP addresses available to dial-in users.	Integer

9.2. IP Pool Example

Pool1	Pool-Status = Enabled,
	Start-Address = "10.2.2.10",
	Range = 4,

This example demonstrates an Enabled IP Pool, starting with the IP Address “10.2.2.10” and ending with the IP address “10.2.2.13” – both inclusive.

10 *Configuring Filters*

The Filtering is implemented in InJoy Connect as plugin feature, described in the Filter documentation included in your InJoy Connect archive.

Filtering in IC is currently per Port Server and not per user, as described in the RADIUS.

11 *Configuring Autostarting*

Auto-starting can automatically start or shutdown applications, REXX scripts or batch files at any of these times:

- port connect
- user-logon,
- IP layer ready,
- user-logoff
- Port disconnect

The autostarting records are linkable from the port records and the user records.

The autostarting attributes and possible values are described in the below table.

11.1.Autostarting Attributes

ATTRIBUTE	POSSIBLE VALUES	DESCRIPTION	TYPE
Description	“string”	This attribute denotes the key or name of the program record. This name must begin in the first position on a new line.	String
Program-Status	Enabled Disabled	Specifies whether the autostarting record is Enabled or Disabled.	Integer
Program	“string”	The path and filename of the executable.	String
Parameters	“string”	The command line options to be passed to the program. Besides normal command line options, the below meta variables are available. Notice that not all meta variables will have meaningful values at all times, so use common sense when picking from the below list.	String
		"[$PORT-ID]"-- Id of port "[$DTE-SPEED]" -- Speed of com-port "[$DEVICE]" – Device name "[$USER-ID]" -- User ID “[$USER-DESCR]” -- User Description "[$PRIORITY]" -- User priority "[$FCS]" -- FCS errors "[$IP-LOCAL]" -- Local IP "[$IP-PEER]" – IP address (PEER) "[$NETMASK]" -- User Netmask "[$PROTOCOL]" -- "PPP" or "SLIP" "[$MTU]" -- MTU of PPP link "[$PKT-OUT]" -- Outgoing Pkts. "[$PKT-IN]" -- Incoming Pkts. "[$CHARS-OUT]" -- Characters Out. "[$CHARS-IN]" -- Characters In "[$CON-TIME]" -- Connection time (secs) "[$IF_NAME]" -- Stack interface name	
Workdir	“string”	The Working Directory of the program to be executed.	String

		For example “d:\os2”.	
Attributes	“string”	A string with extra autostarting options. Currently the only attribute is: “min” to have the program autostarted minimised (if possible).	String

11.1.1. Autostarting Example

PORTCONNECT	ProgramStatus = Enabled,
	Program = "ftp.exe"
	Parameters = "[$IP-PEER]",
	Workdir = "d:\",
	Attributes = "min"

This example demonstrates an autostarting record named “PORTCONNECT” that, when referenced from either a user or port record, will start “ftp.exe” minimised and attempt to connect to the IP address of the dial-in user.

12 *Operating InJoy Connect*

Operating InJoy Connect is simple and straightforward.

This chapter discusses the following topics:

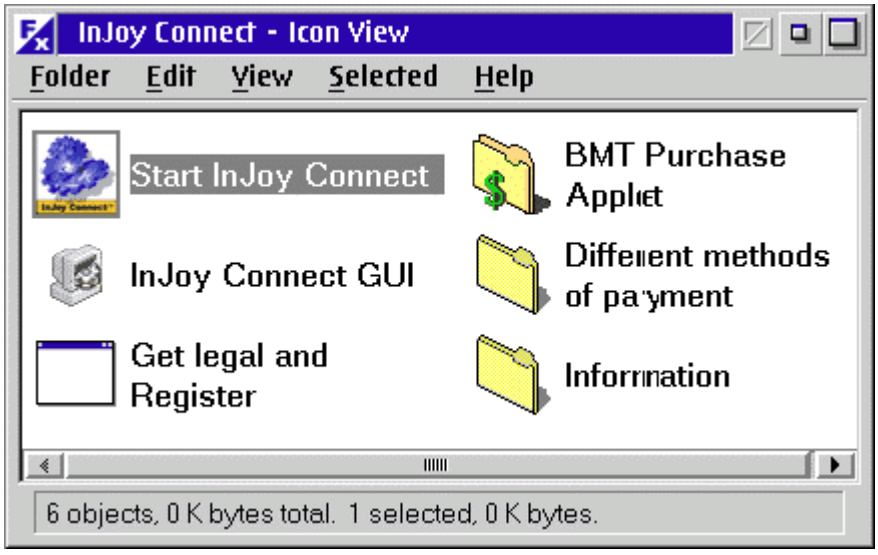
- Starting InJoy Connect
- Selecting a Database Setup
- Putting It Into Action
- Configuration Updates
- Monitoring
- Taking Control

12.1.Starting InJoy Connect

Starting InJoy Connect is a straightforward task and you don't need to configure anything in order for the server to be started. IC requires all modules to be started for successful operation and the distribution archive contains "\bin\run.cmd" to do that job.

12.1.1. Starting The Processes

In the Folder created by "install.cmd", click the "Start InJoy Connect" icon to start the "run.cmd" command file.



When server start-up is complete, you will see 4 new processes on your desktop. The title of all daemon processes are prefixed with "IC:" and as you have read in the IC design section, the processes are vital and they work together to serve your dial-in users.

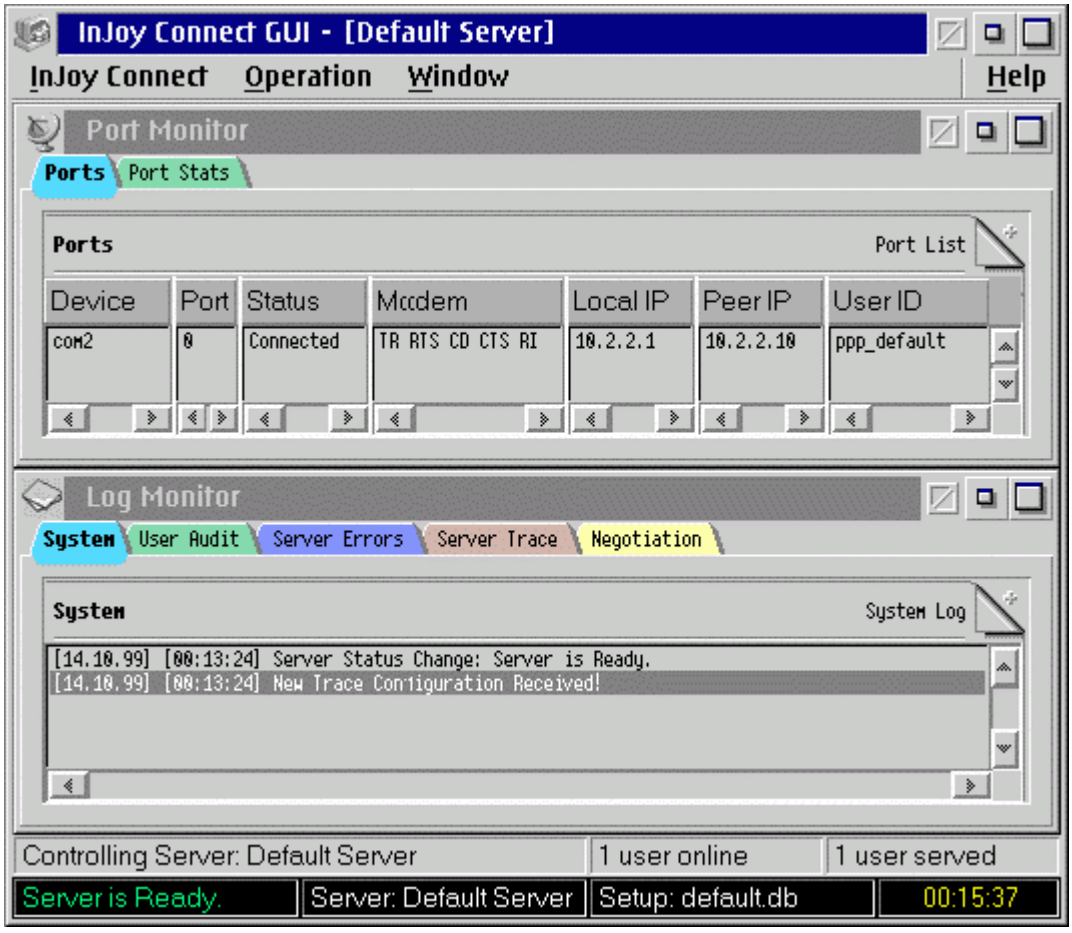
12.1.2. Getting Familiar With The GUI

The "run.cmd" command file will also start the GUI (Graphical User Interface), which should appear on your desktop after a few seconds.

The GUI is a real time monitoring and control tool, whereas configuration of the server parameters is not possible using the GUI. The user interface is customisable and it supports drag and drop of colors of fonts.

With the IC software, it's possible to run several Port Servers and distribute these to remote PCs. The IC GUI can monitor one Port Server at a time and to monitor multiple Port Servers, simply run the GUI in several instances. With several instances of the GUI, you can monitor a whole range of Port Servers and even do remote monitoring of servers via TCP/IP.

The GUI presents itself with simple menus, illustrated below:



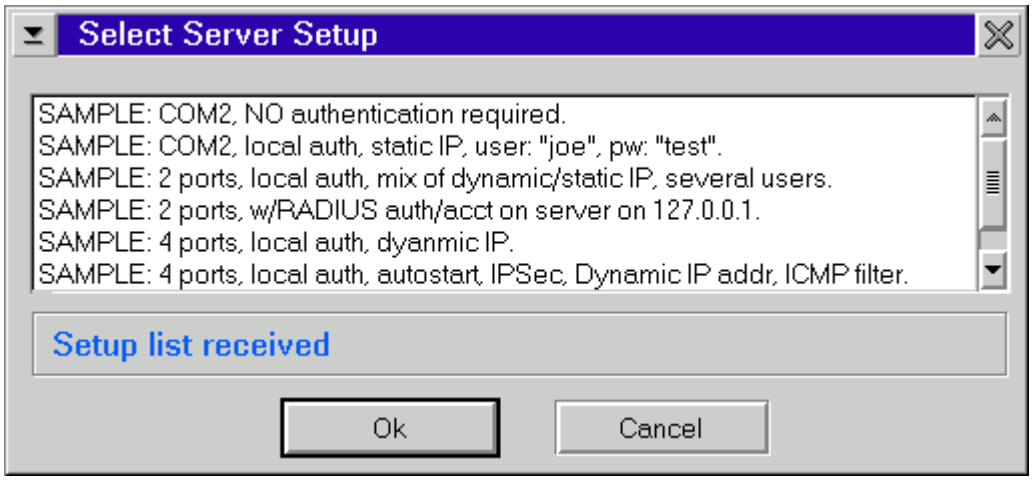
Once the GUI is started, it will search for Port Servers and if it finds more than one, then you will be presented with a dialogue for choosing the server to control.

If only one server is running, then it will be automatically selected for control.

If no Port Servers are operational, then the GUI will start up in idle state and let you choose a database setup.

12.2.Selecting a Database Setup

The GUI allows you to pick a configuration database for your Port Server. The menu for doing this, is found in the "Operation" drop-down and the dialogue presents itself as show below:



The above setups are samples, ready for your modifications.

You will notice that the title of a database setup exactly matches the contents of the ”comment.txt” file located in the matching setup (”.db”) directory. Additionally, when you select one of the setups in the listbox, the little message box will show you the file name of the setup directory.

To get going, simply double-click the desired setup and you are returned to the GUI and ready to put the server into operation. When a Port Server gets the command from the GUI to start serving dial-in users, it will automatically use the configuration from the database you have just selected.

12.3.Putting It Into Action

Having successfully selected a database for the Port Server, you are ready to kick it all into action and start serving dial-in users.

Go to the GUI and to the ”Operation” menu once more. Choose ”Start Server” and you immediately see action as the windows. The trace configurations are updated and ports show up in the port monitor.

Stopping the server is equally simple.

12.4.Configuration Updates

Once you get to serve your first dial-in users, it won’t be long till you need making changes to the configuration files. Maybe you need to add extra ports, extra users or e.g. modify the IP numbers in an IP Pool.

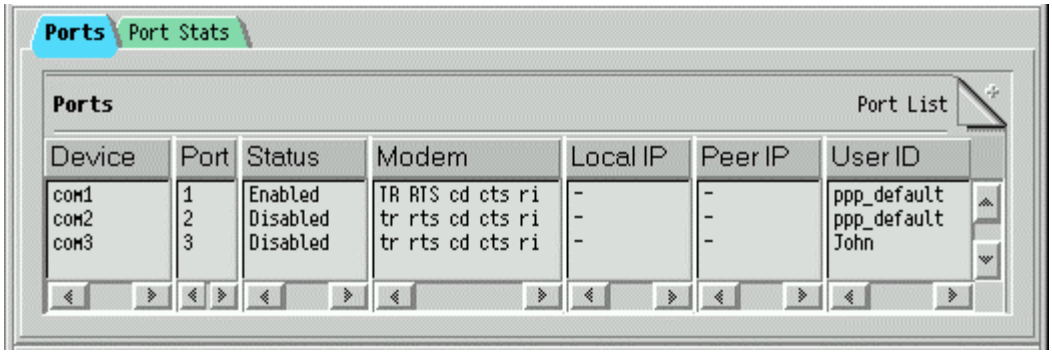
To update the configuration, go to the appropriate configuration files and make your changes.

If you made changes only to the user records, then you don’t need to restart anything, as user records are re-read each time a user logs on.

Changes to the number of ports or other entities, requires you to restart the server. Restarting the server doesn’t mean restart all the software, but it means you need to stop and start the server using the ”Operation” menu in the GUI. Restarting the server that way will force the Port Server to update its configuration.

12.5.Monitoring

Using the GUI, you can monitor port activity and see users as they log on to your server. Two notebook pages are available, each sharing different port statistics for the same ports. The first notebook page is shown below and I don’t think it needs further presentation:

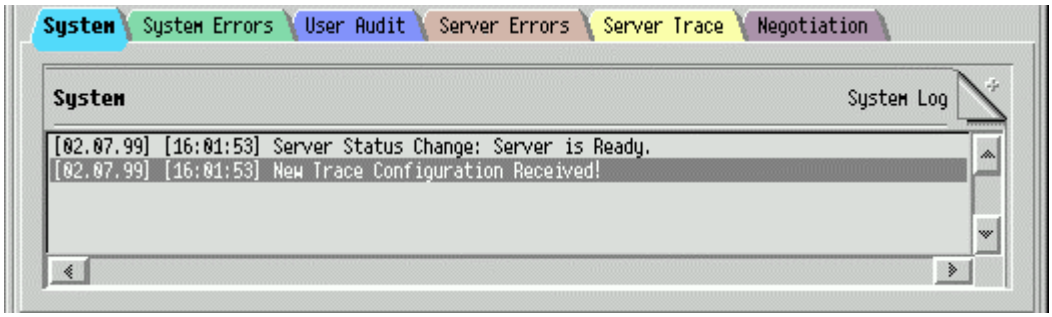


The second notebook tab shows you FCS errors, the port speed and additional port statistics. Looking at it in production is the best way to get acquainted with this window and its usefulness.

Usually the Port Monitor notebook window has a title bar, but if you need to fit this window into the limited room of your desktop, then you can toggle the use of the title bar by pressing ESC.

Below the Port monitor, you will find the Output Monitors. These monitors are fully configurable and extremely powerful for diagnosing any problem, monitoring of system events, tracing and even user auditing.

The figure below shows how the output is divided into configurable notebook pages.

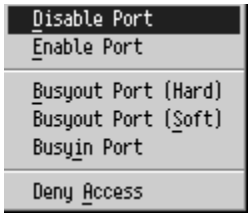


12.6.Taking Control

The Port Servers and the Output Monitors both offer control options.

12.6.1. Controlling Port Status

Right clicking a port in the port monitor brings up the menu shown below.



The menu presents you with a number of actions you can use to control the status of the port. The significance of the actions are as follows:

Disable Port

Disabling the port makes IC drop DTR, send out the modem Disable String, and finally IC releases the port for other uses.

Enable Port
Enables the port by enabling DTR and sending out the modem Init String. When the port appear ”Enabled” in the port list, it means it’s ready to accept new dial-in clients.

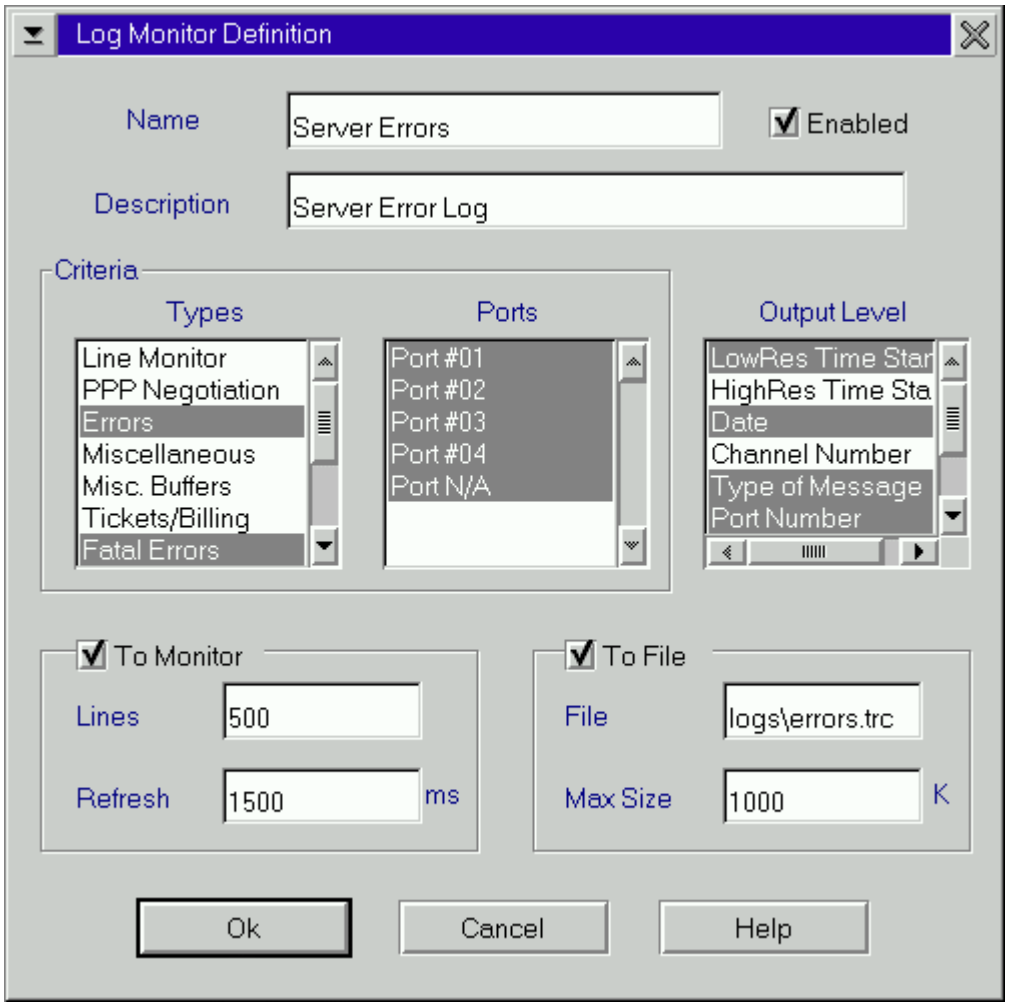
Busyout Port (Hard)
Busyout Hard makes IC drop DTR on the port, effectively dropping the current modem connection. The port remains in IC’s control, but it is not ready for new users till it is busied in or enabled.

Busyout Port (Soft)
Busyout Soft makes IC busy out the port as soon as the current user has logged off.

Deny Access
The Deny Access option is intended to allow dial-in clients to connect, but immediately after connecting, a message will be shown to the user that the system is unavailable. This option is currently of no use as it’s intended for textual logins, which is not yet supported by IC.

12.6.2. Configuring Output Monitors

The comprehensive dialog for logging and tracing customisation allows the system operator to narrowly specify the desired amount of logging. IC ships with a fairly large amount of logging, so when your system runs reliably, you should go into this dialogue and turn off the unneeded logging.



Each notebook-tab (except ”System”) is customisable via the above dialogue and the configuration is really straightforward.

The ”Criteria” is a combination of Log Types and Ports that together form a filter, specifying the information you wish to have in your output monitor and possibly in your log file.

The ”Output level” specifies the amount of information you want to see in the log, i.e. the date, the time, the port number, hex dumps of buffers, etc.

The ”To Monitor” box has options for specifying how many lines of logging you wish to see in the on-screen listbox. Specifying more than 500 lines can slow down your system considerably and refreshing the screen too often will have similar effects.

Logging to a file is optional and in the ”To File” box you specify the file name of the log and the max size in Kilobytes. If you specify a sub-directory for the log file, then be sure to have the directory created up-front, as IC will not do this for you. The path is relative to the active database setup directory. Notice if you don’t specify a path for your log file, then it will be saved directly in the setup directory – together with your ”.cnf” configuration files.

Once done, press OK and your new log tab definition is automatically saved and the on-screen output window is automatically updated with your new output screen. You got to love this feature!

13 *Distributed Computing*

InJoy Connect is a distributed system that can be split up on separate PCs and controlled over the Internet. This chapter discusses the following topics:

- Benefits of Distribution
- Typical Use

13.1. Benefits of Distribution

There are four main reasons for making InJoy Connect a distributed product:

1. Centralised Authentication
2. Centralised Logging
3. Remote Administration
4. Regional Serving

When maintaining larger remote access solutions, then you would want to be able to offer regional dial-in, without having to drive 500 miles each time to want to monitor what goes on at the remote servers.

Regional dial-in became popular when ISPs tried to minimise the cost of Internet access by serving the users where the cost of the connections would be most cost-effective – in the local area. In some regions, the concept of regional servers has been replaced by other technologies, e.g. special phone numbers that are charged at local rate, but really redirects the user to a remote access server. However, in many parts of the world, this type of service is not available and in those cases, the ideal solution is to distribute the modem pools, yet keeping user authentication and management tasks local. That is possible with InJoy Connect.

13.2. Typical Use

Let’s use an example to demonstrate the power of the distributed model.

Assume your company has 6 branch offices that all need to offer remote access for their employees. All employees are known at the company headquarters and some of the employees work in several branch offices at different times. The branch offices are connected via an Internet backbone to the corporate headquarter.

With IC, you would handle the task with this configuration:

Corporate Headquarters
Install IC KERNEL and DBSERV here, together with the configuration database setups. Optionally install a RADIUS server for the user authentication and accounting.

Branch Offices
Install the IC Port Servers and the modems here. One Port Server in each branch office. Connect the Port Servers to the KERNEL running at the corporate building.

Remote Administration and Management
To monitor the individual Port Servers, you can run the IC GUI anywhere, as long as you are connected to the Internet and have an OS/2 handy.

Refer to the Command Line Section to see how you connect the modules over the Internet.

14 *Command Line Options*

InJoy Connect generally doesn't rely on Command Line Options, but a few options are available for connecting modules over the Internet and for auto-selecting database setups.

14.1. Command Line Options Per Module

IC supports the following command line options:

14.1.1. FXKERNEL.EXE

No command line options available!

14.1.2. DBSERV.EXE

-p:password	- For future use
-a:kernel address	- The IP address of the fxkernel module. Default is 127.0.0.1.

14.1.3. PORTSERV.EXE

-p:password	- For future use
-a:kernel address	- The IP address of the fxkernel module. Default is 127.0.0.1.
-s:setup	- Setup directory. Default is "default.db".
-n:server name	- Name of Port Server. Default is "Default Server".

14.1.4. ICGUI.EXE

-p:password	- For future use
-a:kernel address	- The IP address of the fxkernel module. Default is 127.0.0.1.
-s:server	- Server to control. E.g. "Copenhagen Port Server".

Example:
To control an InJoy Connect system running at F/X Communications, you would type:

```
> ICGUI.EXE –a:195.54.80.70
```

15 *Feature Chart*

InJoy Connect will support your efforts to expand the accessibility of your TCP/IP network resources with a collection of high-end features:

15.1. Features by Category

15.1.1. InJoy Connect Base Features

- Believed to be compatible with all major OS/2 TCP/IP packages
- Runs on ANY version of OS/2, newer than Warp 3 Connect.
- Year 2000 ready
- Event triggered start & stop of programs

15.1.2. Robust Dial-In Capabilities

- Support of up to 32 concurrent sessions
- Support for third party port adapters
- Full 32 bit PPP connections (according to the latest RFC's)
- Full 32 bit compressed SLIP connections (according to the latest RFC's)
- Optional CHAP and PAP authentication
- NULL modem support
- Port speeds configurable to 345,600 (hardware and driver permitting)
- Van Jacobson TCP header compression for enhanced performance over dial-up lines

15.1.3. Comprehensive Security

- IPSec VPN support
- Centralised authentication
- PPP CHAP & PAP support
- RADIUS support
- Packet filtering

15.1.4. Centralised management

- Multiple Port Servers
- Central configuration organised into sets
- Central users database
- Central list of ports
- Central configuration of IP-pools
- Central RADIUS accounting
- Central RADIUS authentication

15.1.5. Modularity & Scalability

- Deploy distributed processes
- Deploy geographically dispersed Port Servers
- Deploy extra InJoy Connect Port Servers on the fly
- Maintain multiple database sets
- Start multiple GUI's to simultaneously monitor multiple Port Servers

15.1.6. Graphical User Interface

- Real-time monitoring of remote Port Servers
- Monitor port/modem status
- Monitor connected users
- Enable & disable ports
- Define new log-views and log-files on the fly
- Drag'n'Drop fonts and colors
- Save window position

15.1.7. Logging & Tracing

- Tracing capabilities (including line monitoring)
- Support for the Warp tools 'iptrace' and 'ipformat'
- Trace to screen / file / both
- Centralised logging
- Cached logfile updates - for performance