3Com® IntelliJack® Switch NJ220
User Guide

3CNJ220

www.3Com.com
Part No. 10016226 Rev. AA
Published June 2007

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

TROUBLESHOOTING THE NJ220

TECHNICAL SUPPORT

PRODUCT SPECIFICATIONS

WARRANTY AND REGULATORY INFORMATION

1 INSTALLING THE NJ220 INTELLIJACK

The 3Com NJ220 IntelliJack is a 4-port, managed Ethernet switch that fits into any standard electrical wall outlet or data port opening. It brings switching capabilities to any single port on an Ethernet network by allowing you to connect up to four networking devices, such as computer, printers, and Voice Over IP (VoIP) telephones to the network via one Ethernet port. You can use optional connectors to connect one or two additional devices to separate network segments through the same IntelliJack. All ports feature 10/100 Mbps auto-negotiation.

Power to the IntelliJack is provided through one of the following methods:

- Over the network via an integrated switch that supports Power Over Ethernet
- Over the network via an optional single-port or multi-port Ethernet power supply
- Locally via an optional local power supply

NOTE: Power Over Ethernet, also known as in-line power, is a method to provide power to equipment over an Ethernet cable, allowing a device to receive both data and power from the same network cable. The NJ220 is ideally powered by a switch or other Power Sourcing Equipment (PSE) that is IEEE 802.3af-compatible. The NJ220 can also be powered by some switches which are not 802.3af-compatible. Consult the 3Com web site for more information.

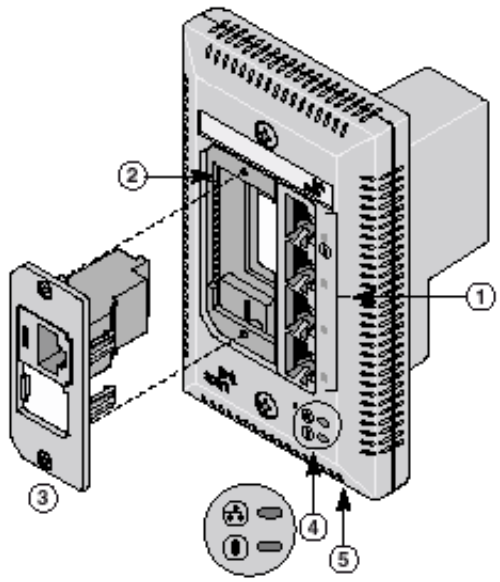
You can manage the NJ220 IntelliJack using the included Central Configuration Manager or Web Configuration Manager. You can also use a supported SNMP management console as you would with any managed device on your network, but greater management and control is available through the Configuration Manager software. Management features include:

- Device discovery
- Port status (state, duplex, speed)
- Statistics
- Port control (port state, flow control, AutoMDI(X), frame rate limit)
- 802.1P QoS/Priority
- 802.1Q compatible VLAN
- VLAN tag add/remove
- Firmware upgrade
- Rate limiting

- MAC filtering
- 802.1x port security
- User-configured VLAN IDs for management packets
- Port-based "calendar" function

About the IntelliJack

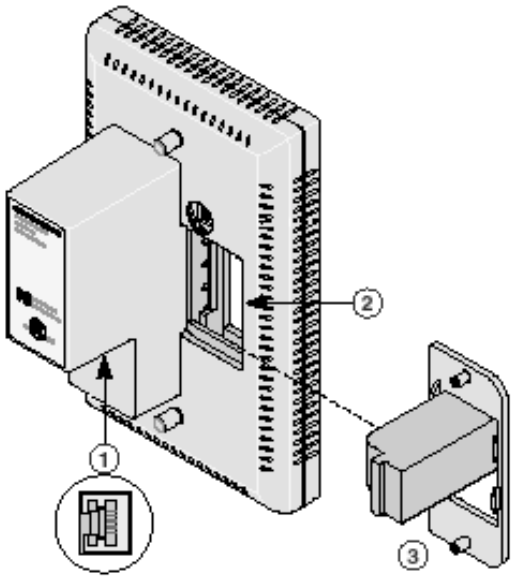
The following diagram shows the front view of the IntelliJack:



1	Switched ports with LEDs	Allow up to four devices to be connected to the network. A green LED indicates connection status when a device is using a particular port. Port number 1 is also a power-forwarding port; it can be used with any standard networking device as well as to power a VoIP telephone on a network that uses IEEE 802.3af-compatible Power Over Ethernet. An additional LED indicates when the port is forwarding power to a device connected to that port.
2	Slot for adapter plate	Can be fitted with an adapter plate, which can be installed with up to two pass-through ports.
3	Adapter plate with installed pass-through port connector	Can be used for voice or other networking applications. The port bypasses the functionality of the switch, allowing you to set up a connection to a separate network segment or to connect to an analog or digital PBX telephone. The adapter plates are available from 3Com. However, you must purchase the connectors from the manufacturer. See "Installing the Adapter Plate and Pass-Through Ports" on page 8 for more information.

4	LEDs	Indicates network connection status. Indicates power status.
5	Power socket	Can be used to power the IntelliJack with a local power supply (available for purchase from 3Com); required if your network does not support Power Over Ethernet.

The following diagram shows the back view of the IntelliJack:



1	Ethernet uplink port (RJ-45 female)	Connects the IntelliJack to the network. Make sure the port on the network switch to which the IntelliJack is connected is configured as a standard MDI-X port.
2	Slot for adapter plate	Can be fitted with an adapter plate, which can be installed with up to two pass-through ports.
3	Adapter plate with installed pass-through port connector	Connects the installed pass-through port to the network.

Before You Begin

Before you begin installation, register your product at: http://eSupport.3com.com/.

The IntelliJack is available in single- and 20-packs. Before you begin the installation, make sure you have the following items, which are included with the IntelliJack:

- 1.5 inch, 6x32 screws (2 per IntelliJack) for mounting the IntelliJack to the wall or office cubicle.
- Male to male RJ-45 coupler cable (1 per IntelliJack) for connecting the Ethernet cable from the network to the IntelliJack (required only if your network cable is terminated with a female RJ-45 connector).

Additionally, the following items are shipped with the single pack:

- Compact disc with User Guide and Configuration Manager software.
- Adapter plates for installing connectors to use as pass-through ports. The adapter plates accommodate connectors from suppliers including:
  - Panduit (RJ-45 and RJ-11)
  - Avaya (RJ-45 and RJ-11)
- Adapter plate screws (2) for mounting the adapter plate to the IntelliJack.

NOTE: The connectors for the adapter plates must be purchased from the manufacturer. For a list of supported connectors, go to the IntelliJack section of www.3com.com/.

Obtaining Optional Components

The IntelliJack works with the following optional components, all of which are available from 3Com. Order online at www.3com.com or by calling 1-877-949-3266.

Component	Purpose	3C Number(s)
Adapter plates	For installing pass-through port connectors of your choice that allow a direct connection to another network segment or for connecting an analog or digital PBX telephone. Available adapter plates accommodate connectors for the following manufacturers: AMP, Avaya, Hubbell, Ortronics, and Panduit.	3CNJAP-PA-20 3CNJAPB-PA-20 3CNJAP-AV-20 3CNJAPB-AV-20 3CNJAP-AM-20 3CNJAPB-AM-20 3CNJAP-HU-20 3CNJAPB-HU-20 3CNJAP-OR-20 3CNJAPB-OR-20
Single-port Ethernet power supply	For providing Power Over Ethernet to locally power a single IntelliJack.	3CNJPSE
Multi-port Ethernet power supply	For providing Power Over Ethernet to power up to 24 IntelliJacks.	3CNJPSE24 3C17205

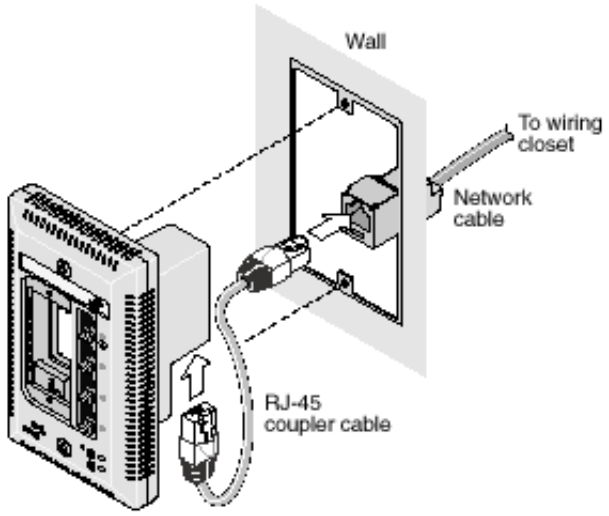
Component	Purpose	3C Number(s)
Local power supply	For locally powering a single IntelliJack; required if your network does not support Power Over Ethernet.	3CNJPSL
VoIP telephone power cable	For powering a VoIP telephone on a network that uses Capacitive Power Discovery Process-compatible Power Over Ethernet.	3CNJVOIPMOD-NBX 3CNJVOIPMOD-20 3CNJVOIP-CPOD 3CNJVOIP-CPOD-20
Extension ring	For ensuring that the IntelliJack is properly mounted to a cubicle; required if the cubicle opening: ▪ Has a depth of fewer than 1.5 inches. ▪ Does not support the NEMA-WD6 standard. ▪ Does not have pre-drilled screw holes for standard mounting.	3CNJEXTRING

Installing the IntelliJack

Installing the IntelliJack consists of the following steps:

1. Set up the power supply (page 6).
2. Install the adapter plate and pass-through ports (page 8).
3. Plan the installation (page 9).
4. Set up the network cabling at your site (page 10).
5. Connect the IntelliJack to the network (page 10).
6. Mount the IntelliJack to the wall or office cubicle (page 11).
7. Connect the local power supply (page 12; optional) not required if your network supports Power Over Ethernet or if you are using a single-port or multi-port power supply).
8. Connect network devices to the IntelliJack (page 13).

The following diagram displays an overview of the recommended installation, where the IntelliJack is being connected to an Ethernet network cable that is terminated with a female RJ-45 connector. Detailed installation instructions are included in the sections that follow.



Setting up the Power Supply

Power to the IntelliJack can be supplied one of the following ways:

- Over the network via an integrated switch that supports Power Over Ethernet.
- Over the network via a multi-port Ethernet power supply.
- Over the network via a single-port Ethernet power supply.
- Locally via a 3Com local power supply.

Before you begin the installation, determine which type of power supply the IntelliJack will use.

NOTE: For a list of power supplies that support the IntelliJack, go to www.3com.com/.

CAUTION: Use only a power supply that is provided or approved by 3Com for use with this IntelliJack. Failure to do so may result in damage to the IntelliJack, or may result in a hazardous situation or personal injury.

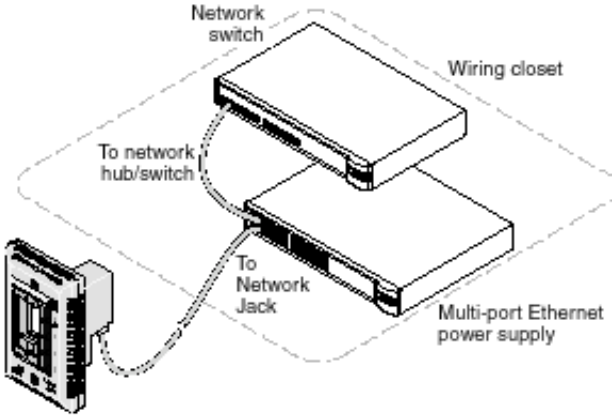
Using an Integrated Switch with Power Over Ethernet

To use Power Over Ethernet, you must have a switch on the network that has Power Over Ethernet integrated into it. You must then determine if it is compatible with IEEE 802.3af.

Using a Multi-port Ethernet Power Supply

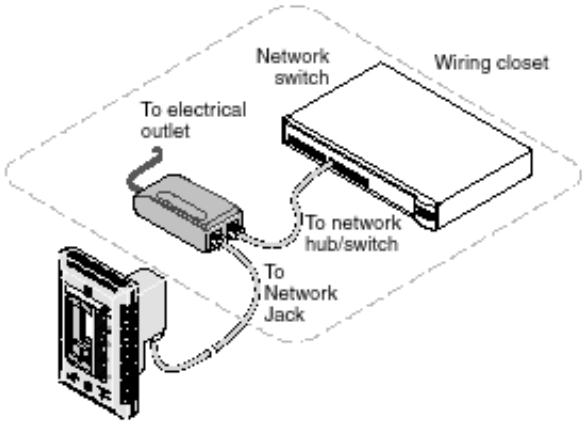
To use a multi-port Ethernet power supply, you must connect the power supply to your network, as shown in the illustration.

The multi-port Ethernet power supply from 3Com connects to an existing Ethernet or Fast Ethernet infrastructure with standard Category 5 or Category 5e UTP cabling, and powers up to 24 IntelliJacks. See "Obtaining Optional Components" on page 4 for ordering information. For complete installation instructions, see the multi-port Ethernet power supply documentation.



Using a Single-port Ethernet Power Supply

To use a single-port power supply, connect the power supply to the network hub or switch and to the IntelliJack, as shown in the following illustration. See "Obtaining Optional Components" on page 4 for ordering information. For complete installation instructions, see the single-port Ethernet power supply documentation.



Using the 3Com Local Power Supply

To use the local power supply, make sure you have an electrical outlet near the site where the IntelliJack will be installed. First plug the power cord into the IntelliJack, then plug it into the electrical socket. See page 12 for more details.

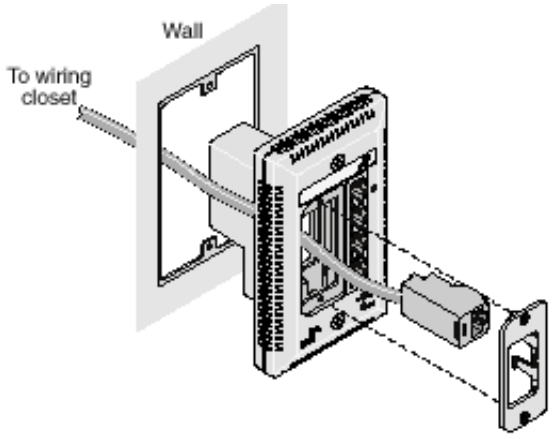
Installing the Adapter Plate and Pass-Through Ports

Install the blank adapter plate, or if you want to use pass-through ports for connecting an analog or PBX digital telephone or for setting up a connection to a separate network segment, purchase supported connectors and install them on the appropriate IntelliJack adapter plate (included with the single pack; available for purchase separately with the 20-pack).

For a list of connectors that are supported with the IntelliJack adapter plates, as well as any corresponding installation instructions, go to the IntelliJack section on www.3com.com.

NOTE: If you are not planning on installing the adapter plate and pass-through ports, skip this section. Go to "Planning the Installation" on page 9 to begin the installation.

1. Pull the network cable(s) from the wiring closet to the location of the IntelliJack.
2. Thread the network cable(s) through the empty slot on the IntelliJack.



3. Terminate the end of the network cable(s) with the connector(s) you purchased separately.

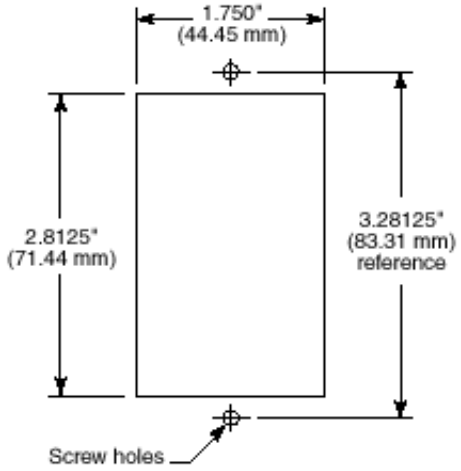
   Refer to the connector manufacturer's instructions for terminating the cable. Be sure to test end-to-end system functionality and verify that it is working.
4. Snap the connector(s) into the appropriate adapter plate.

   Each adapter plate is labeled with the name of a connector's manufacturer. Be sure to use the adapter plate that matches the manufacturer of your connector(s).
5. Mount the plate to the IntelliJack using the two adapter plate screws provided.

Planning the Installation

When installed, the back of the IntelliJack extends into a wall or cubicle opening 1.5 inches. Because the depth of some wall and cubicle openings differ, observe the following requirements and recommendations before installing the IntelliJack:

- Make sure the wall or cubicle opening where the IntelliJack is being installed complies with the NEMA-WD6 standard, as described below.



- Make sure the distance between the back of the IntelliJack and the inside of the wall or cubicle opening is at least 1.5 inches (3 inches is recommended).

NOTE: Some cubicle openings have a depth of 1.2 inches. In this case, install the IntelliJack using the extension ring (available for purchase separately; see "Obtaining Optional Components" on page 4) to obtain the minimum 1.5-inch depth.

If installing into a wall junction box, make sure there is enough space between the back of the IntelliJack and the inside of the junction box to maintain an acceptable bend radius on the cable. If you encounter interference or need additional clearance between the IntelliJack and where it sits inside the junction box, use the extension ring.

- To ensure proper horizontal cabling functionality, adhere to the following network cabling standards during installation:
  - ANSI/TIA/EIA-568
    Commercial Building Telecommunications Cabling Standard
  - ANSI/TIA/EIA-569
    Commercial Building Standard for Telecommunications Pathways and Spaces

Setting up the Network Cabling at Your Site

The network cabling at your site (from the wiring closet to the wall or cubicle opening) may already be installed. If it is not, install the cabling following these general guidelines.

CAUTION: It is recommended that a professional cable installer performs these procedures. Be sure to adhere to local safety and regulatory codes during the cable installation.

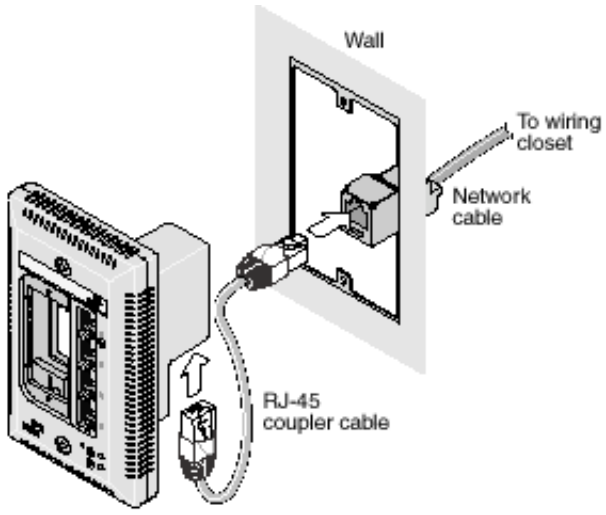
1. Connect one end of an Ethernet cable to your network. Usually, this connection is done in a network wiring closet, via the patch panel.
2. Terminate the other end of the cable at the location where the IntelliJack is being installed (using either a female or male RJ-45 connector).

   Refer to the connector manufacturer's instructions for terminating the cable. Be sure to test the connector and verify it is working.

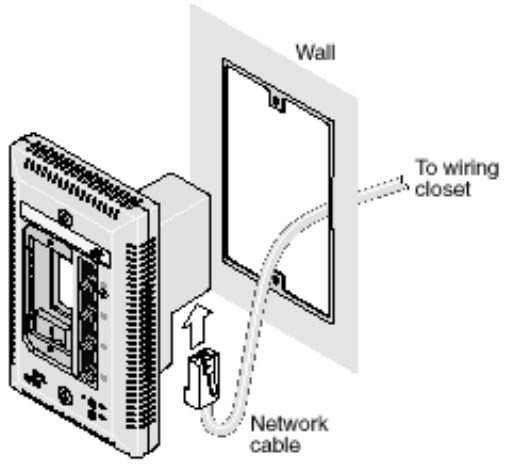
Connecting the IntelliJack to the Network

The method for connecting the IntelliJack to the network is determined by how your network cable is terminated (as described in the previous section, "Setting up the Network Cabling at Your Site").

- If the end of the cable is terminated with a female RJ-45 connector, use the RJ-45 coupler cable included in the package to connect the IntelliJack to the network cable (recommended installation.)



- If the end of the cable is terminated with a male connector, connect the network cable directly into the Ethernet uplink port.

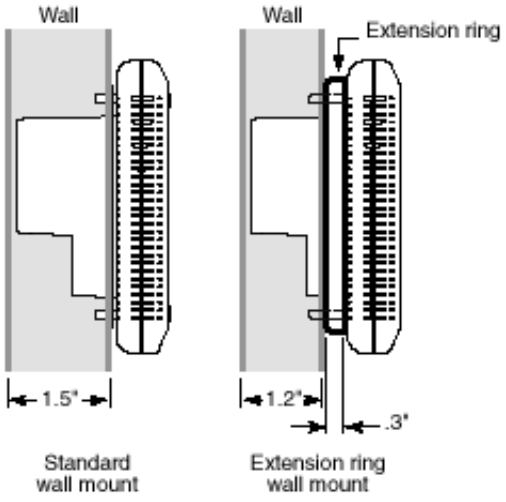


Mounting the IntelliJack

After connecting the IntelliJack to the network, use the two provided screws to mount the IntelliJack in any standard NEMA-WD6 cubicle opening or wall outlet.

If the cubicle or wall opening has a depth of fewer than 1.5 inches, does not support the NEMA-WD6 standard, or does not have pre-drilled screw holes, mount the IntelliJack using the extension ring, as shown below.

NOTE: The extension rings are designed to stack on top of one another. If you need more than 0.3 inches of clearance, simply snap an additional extension ring to the back of the IntelliJack.

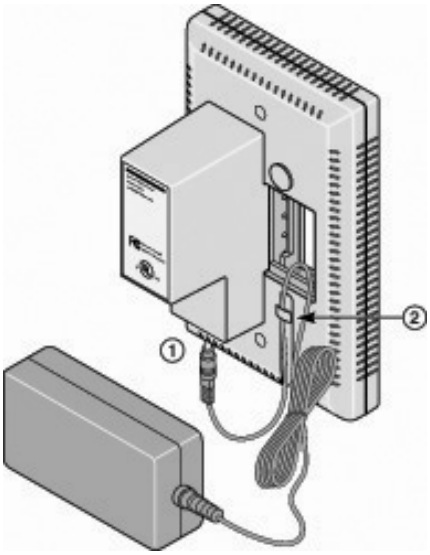


CAUTION: Make sure the vents along the edges of the IntelliJack faceplate are clear of any obstructions. If necessary, install the extension ring on recessed openings to allow airflow to vents.

Connecting the Local Power Supply (Optional)

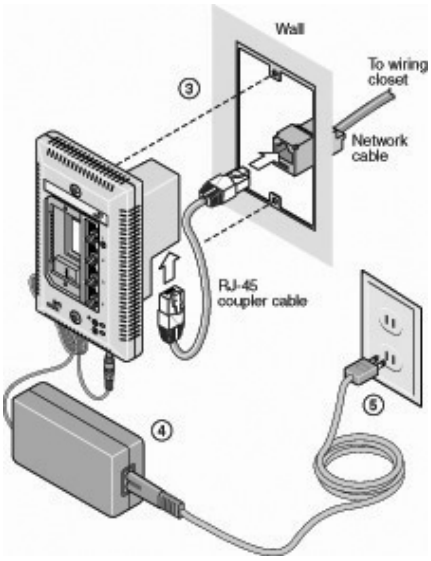
If your network does not support Power Over Ethernet, or if you are not using a single-port or multi-port Ethernet power supply, you must purchase a local power supply from 3Com (see "Obtaining Optional Components" on page 4). To connect the local power supply to the IntelliJack, please follow these steps:

1. Route the power cable through the strain relief of the IntelliJack (as shown in the diagram below).
2. Securely mount the IntelliJack on a wall.



3. Plug the power cable into the IntelliJack.
4. Secure the local power supply and cable to the wall.

5 Plug the local power supply into the power source.



WARNING: Use the local power supply available from 3Com. Failure to do so may result in damage to the IntelliJack, or may result in a hazardous situation.

Connecting Devices to the IntelliJack

After the IntelliJack is installed and mounted, connect your networking devices (such as computers, printers, etc.) to any of the four switched ports on the front of the IntelliJack.

If you installed the adapter plate with pass-through ports, connect the appropriate device(s) to the port(s).

Checking the LEDs

You can verify the IntelliJack installation by checking the LEDs.

LED	Description
(LAN)	▪ On—The IntelliJack is connected to the network and a link has been established. ▪ Off—There is no connection to the network.
(Power)	▪ On—The IntelliJack is receiving power (local or via the network). When you first connect power to the IntelliJack, there will be a delay of approximately 5 seconds. The power LED light will blink several times before remaining solid on. ▪ Off—The IntelliJack is not receiving power.

Additionally, each of the switched ports has a green LED which lights when a device is connected. Port 1 also has an amber LED which lights when the IntelliJack is forwarding power to a connected device.

2 INSTALLING THE CONFIGURATION MANAGERS

Once you have installed the NJ220 hardware, you need to configure it for use on your particular network. To configure the NJ220, install the Local and Central Configuration managers.

NOTE: You will use the Local Configuration Manager for initial configuration of the NJ220 on your network. It's usually easiest if you load this software on a laptop and use it to configure IntelliJacks as you install them.

The NJ220 Central Configuration Manager is used for advanced configuration and management of one or more NJ220s on your network. This software should be installed on the machine you plan to use to manage your NJ220s from a remote location—perhaps the same console you use for SNMP management.

System Requirements

The machine you install the software on should meet the following requirements:

- Pentium processor
- Minimum of 15MB disk space
- Windows 2000, Windows XP Pro, or Windows NT 4.0 with Service Pack 6 installed (While Windows 95 and Windows 98 are not recommended operating systems for use with management platforms, the Configuration Manager software may work with them) or Windows Vista.

Installing the Local and Central Configuration Managers

Run the following steps to install the Configuration Manager software:

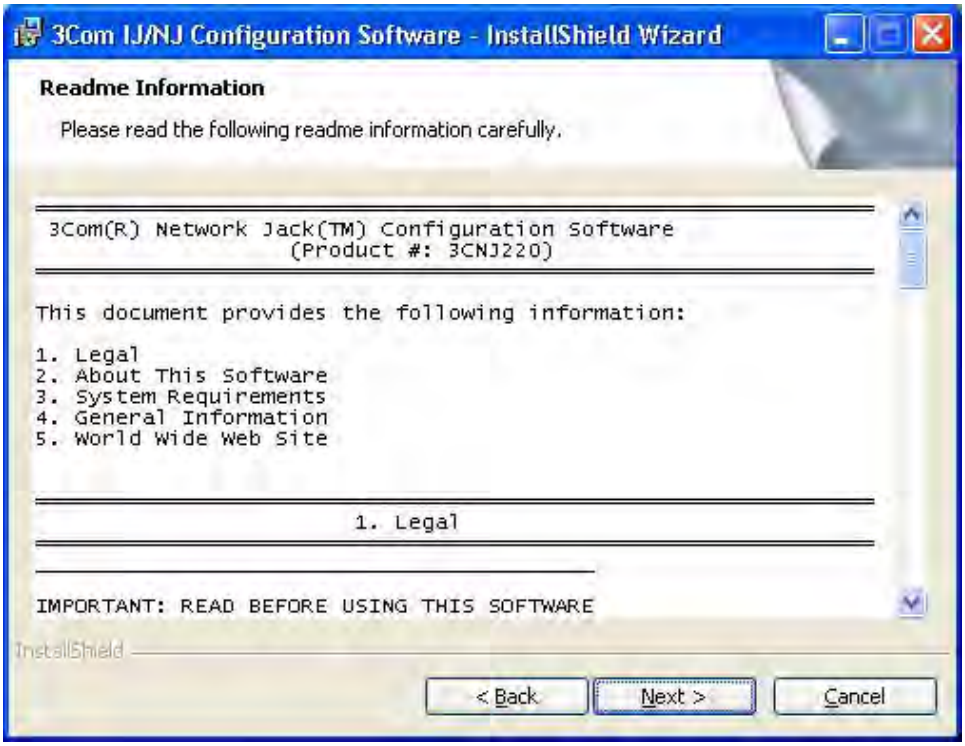
1. Insert the Configuration Manager software CD into your Windows 2000, Windows XP Pro, Windows NT, or Windows Vista computer.

2 If your computer is configured to Auto-Play CDs, the installation will start automatically. If not, double-click the setup.exe icon on the CD, and you will see this window:

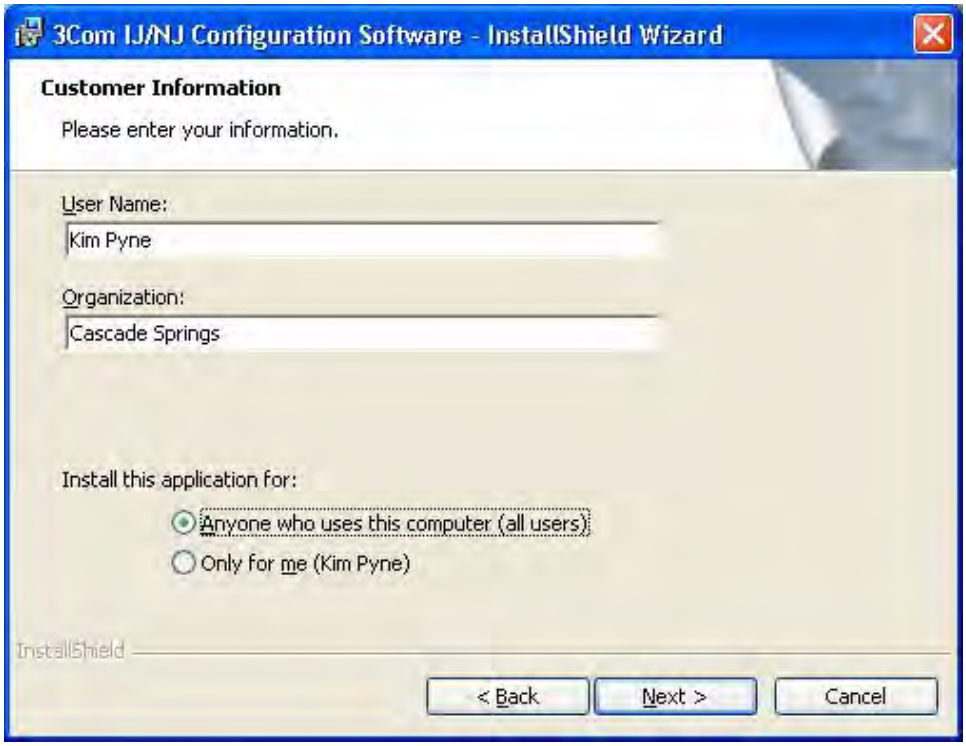
3 Click Next to continue.

4 Carefully read the license agreement. If you agree, click "Yes, I accept" and Next to continue.

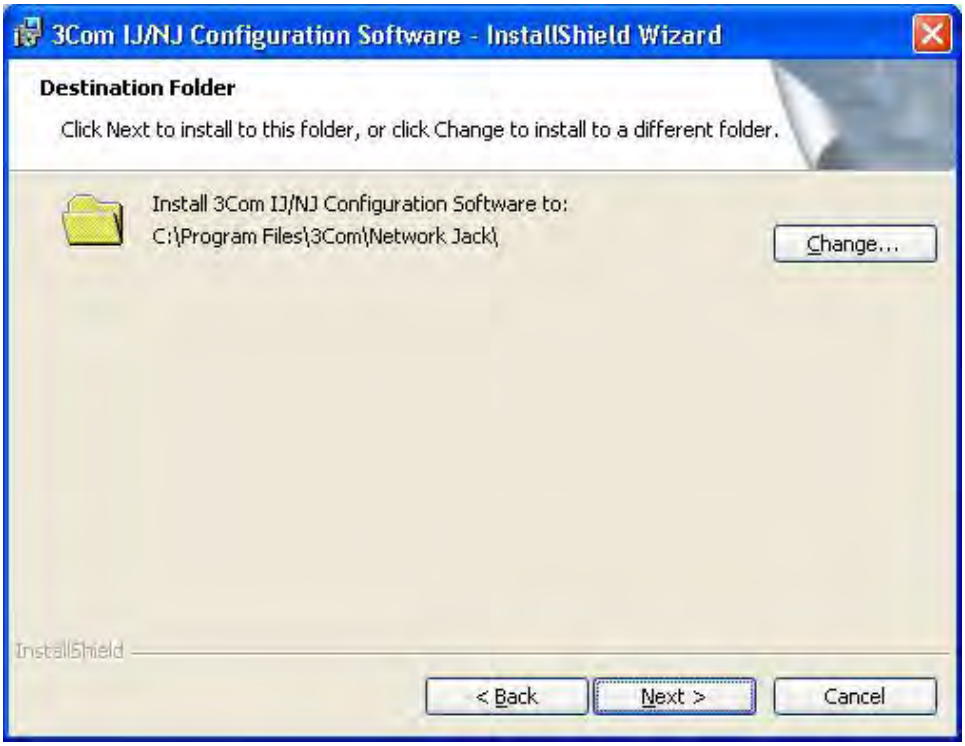
5 The installation will present Readme Information. This is also found in the Readme.txt file on the installation CD. Please read the information and click Next to continue.



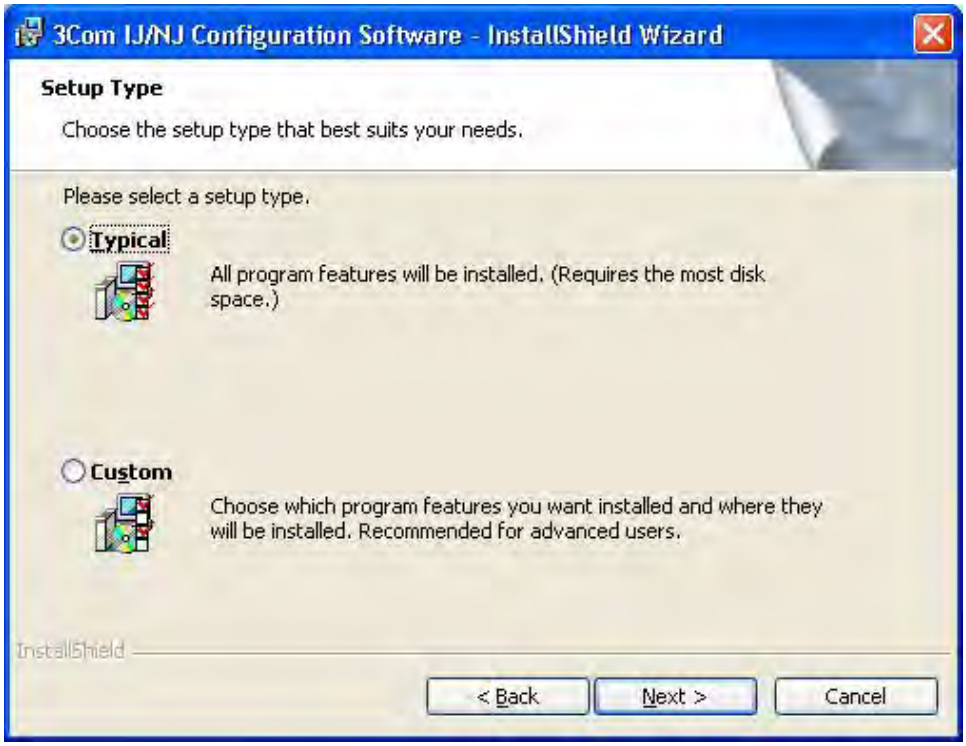
6 Enter your user and organization names. You can also specify whether you want the management programs to be available to just you or to anyone that may use the computer you're installing these applications on. Select the option you prefer and click Next.



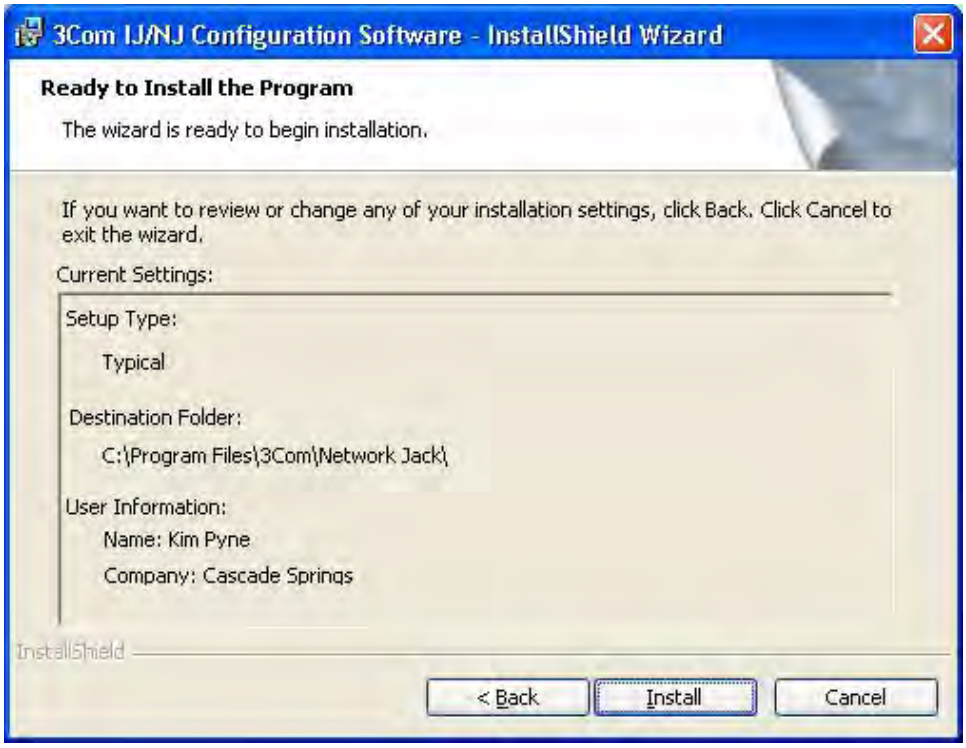
7 The program files will be installed in the directory C:\Program Files\3Com\IntelliJack. If you want to change the location of the installation, click Change. Otherwise click Next to accept the default location and continue.



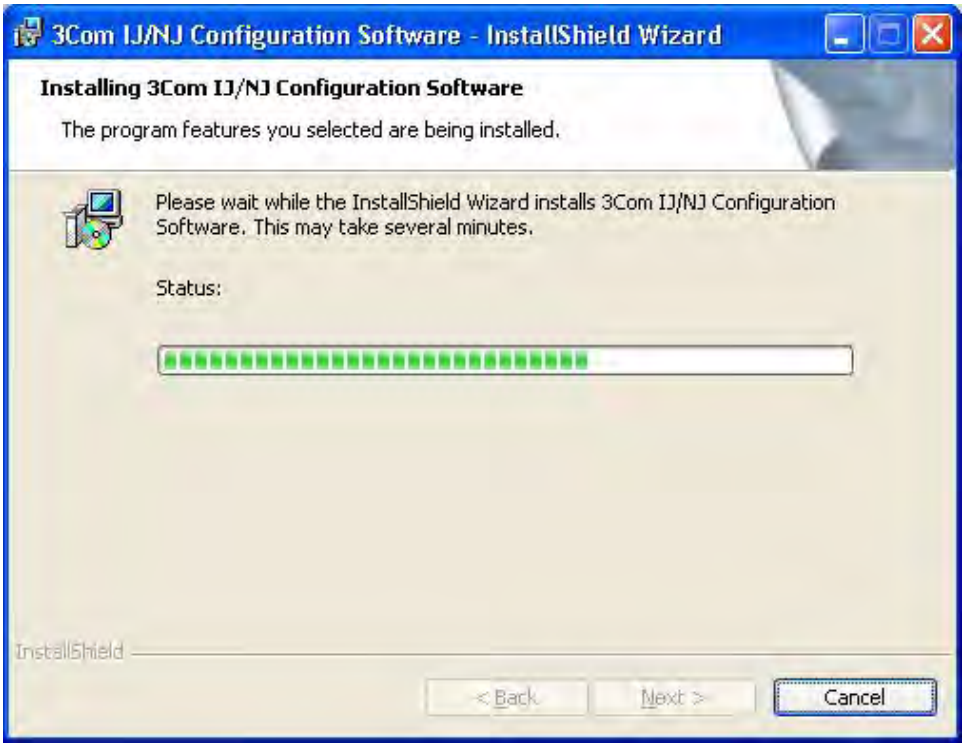
8 Select a typical or custom setup and click Next. The Typical installation will install both the Local Configuration Manager and the Central Configuration Manager on your system. The Custom installation option lets you install just one of the programs if you wish.



9 Review the settings you selected and click the Install button.



10 When the installation has completed, click the Finish button to close the installation utility.



The installation utility will create two shortcut icons on the Desktop--one for the Local Configuration Manager and one for the Central Configuration Manager.

You can also launch the programs from a program group you can access from the Start menu. The program group folder is labeled 3Com IntelliJack and can be found under the Programs menu.

Installing the Web Configuration Manager

NJ220 IntelliJacks are capable of being discovered and managed through a standard web browser. The Web Configuration Manager lets you access and control IntelliJacks from any Web-enabled computer on your network.

In order to enable the Web Configuration Manager you will need the following:

- A servlet-compliant web server or stand alone servlet engine
- Internet Explorer 6.0 or later; Netscape 7.0 or later web browser
- NJ220 Installation CD

The following instructions assume a scenario where the operating system being used is Microsoft Windows 2000 and the servlet engine is Apache Tomcat, Version 4.1. You may have to slightly alter this process if your specific environment is different. Note that Apache Tomcat requires Sun Microsystems' Java Development Kit (JDK) 1.4. These are available at no charge from Sun.

To install the 3Com IJ/NJ Web Configuration Manager on a Windows 2000 computer, follow these steps:

1 If your machine does not have the Java Development Kit (JDK) installed, download the installation program from Sun's Web site and install JDK v1.4. You can find JDK 1.4 at the following URL:

http://java.sun.com/

Scroll down the to the "Download J2SE v 1.4.2" section and choose to download the SDK executable file for Windows installation. Do not choose the JRE executable file.

NOTE: Make a note of the directory in which you install the JDK.

NOTE: This file is approximately 150 MB. At the time of download, Sun will tell you the amount of hard drive space this file requires. Make sure you have the required space before proceeding.

2 If your machine does not have the Apache Tomcat servlet engine, download the installation program from the Apache web site and install Tomcat on your machine. We currently recommend that you install Version 4.1.27 of Tomcat. You can find the Apache Tomcat servlet engine at the following URL:

http://jakarta.apache.org/site/binindex.cgi

Scroll down to the 'Tomcat' section and download the '4.1.27.exe' file.

NOTE: Make a note of the directory in which you install this program.

3 You need to set the 'JAVA_HOME' environment variable to the directory where you installed the JDK. To set this variable on Windows 2000, go to the Start menu and select Settings>Control Panel>System>Advanced>Environment Variables. Under System Variables section on the Advanced tab, click New. In the dialog box that appears, enter JAVA_HOME in the "variable home" field and the directory path to the JDK in the "variable value" field. Click OK.

4 Copy the 'CB.DLL' file from the NJ220 Installation CD into the Windows system directory (C:\WINNT\SYSTEM32).

5 Copy the 'buildDirs.bat' file from the NJ220 Installation CD to the root directory of the drive in which you installed Tomcat.

For example, if you installed Tomcat in the C:\Tomcat directory, copy buildDirs.bat to the C:\ directory.

6 Open a DOS command window, navigate to the directory in which you copied the 'buildDirs.bat' file, type 'buildDirs.bat' and press Enter. At this point, the following directory structure will be created: c:\3comnjwbm.

7 Copy the 3ComIJNJ.war file from the NJ220 Installation CD into the 'webapps' subdirectory under the Tomcat installation directory. For example, if you installed Tomcat in the C:\Tomcat directory, copy 3ComIJNJ.war into the C:\Tomcat\webapps directory.

8 If the 'webapps' subdirectory under the Tomcat installation directory already contains a subdirectory called '3ComIJNJ,' delete this directory.

9 Start Apache Tomcat. To do so, open a DOS command window, go to the 'bin' subdirectory under the Tomcat installation directory, type 'startup', and hit Enter. A new command window will open. At this point, your server should be configured and running.

Now that your server is configured, you can use the Web Configuration Manager from any Web-enabled machine. To do so:

10 Open up your Internet Explorer or Netscape browser and point it to the following URL:

http://<Your_Server_IP_Address>:8080/3ComIJNJ/main/index.jsp

3 USING THE LOCAL CONFIGURATION MANAGER

Initializing the NJ220 IntelliJack

Once you have installed the NJ220 hardware on your network and the Local Configuration Manager software on your computer, you need to perform an initial configuration of the IntelliJack.

1. The first step is to connect your computer to the NJ220 that you are installing. Attach an Ethernet cable from a computer running the Local Configuration Manager software to any one of the four personal area network (PAN) ports on the front of the NJ220.
2. Click on the desktop shortcut icon labeled IJ NJ Local Config Mgr to start the program. When it launches, you will see a window like this:

3. The MAC address, Serial Number, and Firmware Version of the currently connected NJ220 will appear at the top of the window. If you connect to another NJ220, you must click the Query button to refresh the window.

   If you are not connected to any IntelliJack, the field will display the message Not Connected. If the Not Connected message appears, check your connection to the IntelliJack and click the Query button.
4. Make sure the General tab is selected.

5 Enter Location Information for the NJ220 you are currently configuring. This field can help you and other network managers identify this IntelliJack in the future. You may enter any information you like (up to 128 characters), but we recommend that you enter a logical, easy to follow description, such as "Building A, 3rd floor, room 315, West wall."

6 Enter a Group Name for this IntelliJack. This can be any name you wish. With the Central Configuration Manager, you can perform management tasks on all IntelliJacks with the same group designation.

7 Select the method the NJ220 should use to obtain an IP address. The NJ220 can either get an IP address from an existing DHCP server on your network, or you can specify an address. If you elect to specify your own address, you should enter the IP Address, Subnet Mask, and Default Gateway information in the appropriate fields.

NOTE: By default, the NJ220 is configured to automatically obtain an IP address from a DHCP server. If no DHCP server exists, or if the NJ220 cannot obtain an IP address, it will default back to its previously configured static IP address. If it had previously been assigned an IP address, it will default to that one. If it did not, it will default to the static IP address of 192.168.1.252.

8 If you wish, check the box next to Lock IP Address. Selecting this option will ensure that the IntelliJack will always use a particular address.

WARNING: If you lock an IP address and reserve it for this IntelliJack, make sure you configure your DHCP server so it won't distribute that address to other devices.

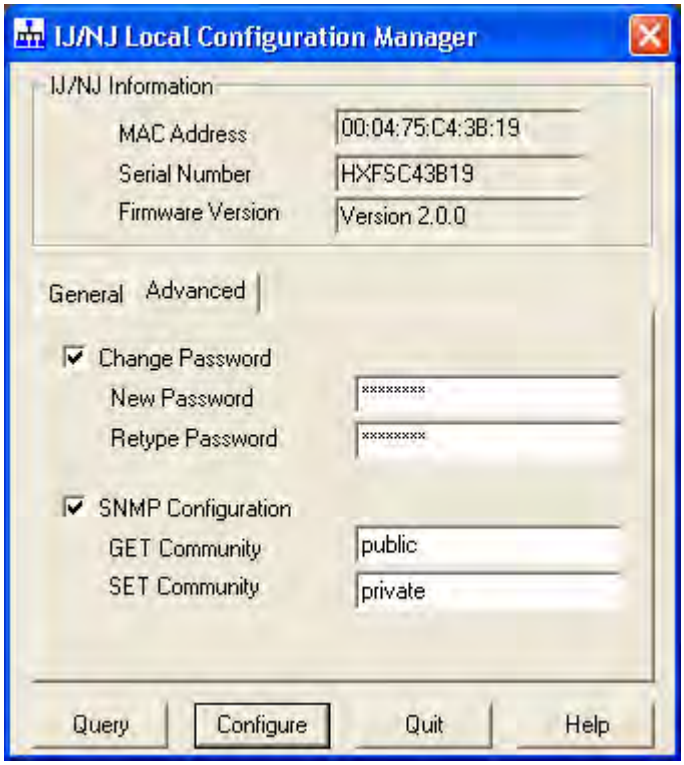
9 Click the Configure button and the Local Configuration Manager will ask you to enter the password for the device. If you haven't changed the password, you should enter the default password, which is "**password**" (without the quotes). Your changes are sent to the NJ220 and will become effective immediately.

Those are the only steps *required* to initialize your NJ220 IntelliJack.

Setting Advanced Options

If you want to change the default password of the NJ220 or change SNMP community strings, you can configure these settings from either the Local Configuration Manager or the Central Configuration Manager (covered in the next chapter). In the Local Configuration Manager, both settings are found under the Advanced tab.

1 Select the Advanced tab on the IntelliJack Local Configuration Manager window.



2 To change the IntelliJack's configuration password, click on the box next to Change Password. Then enter the new password in both password fields. (You must enter the password twice to ensure you type it correctly.) The password you select can be any combination of letters and numbers between 8 and 32 characters.

3 To configure the NJ220 for management with an SNMP console, select the SNMP Configuration box. Enter the GET Community string and SET Community string in the appropriate fields. Each field lets you enter any combination of letters and numbers up to 32 characters.

4 Click the Configure button and the Local Configuration Manager will ask you to enter the password for the device. If you haven't changed the password, you should enter the default password, which is "**password**" (without the quotes). Your changes are sent to the NJ220 and will become effective immediately.

NOTE: You should change the password to ensure that no one else can re-configure your system. Make sure you remember the new password you set. ***If you forget the new password, you will not be able to perform any other configuration tasks unless you send the device back to 3Com****.*

4 USING THE CENTRAL CONFIGURATION MANAGER

You should use the Local Configuration Manager to initialize each of the NJ220 IntelliJacks installed on your network. Once you have completed that step, you can manage all of them with the Central Configuration Manager.

Install this program on any computer on your network you want to use as a central management console (See chapter 2, "Installing the Configuration Managers" for help). You can use the same machine that has your SNMP-based management platform. The Central Configuration Manager will be able to configure and manage all of the IntelliJacks that reside on your network.

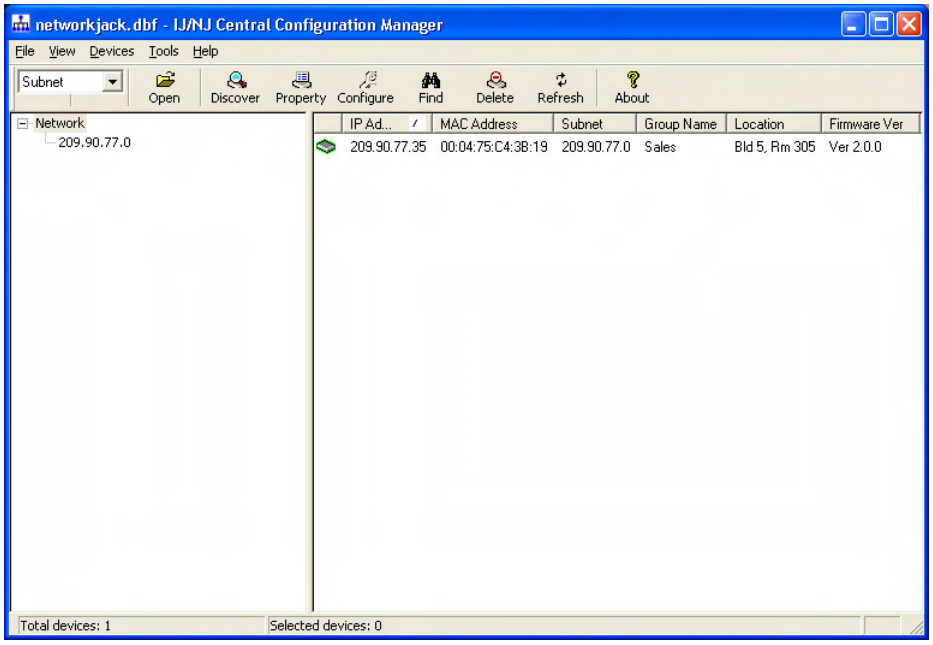
We recommend that you keep the Central Configuration Manager (CCM) running on your machine. Information such as traps and alerts are sent tot he CCM on a periodic basis. If you shut off the machine or close the configuration manager, you will not be able to receive this information.

Discovering NJ220 Devices on Your Network

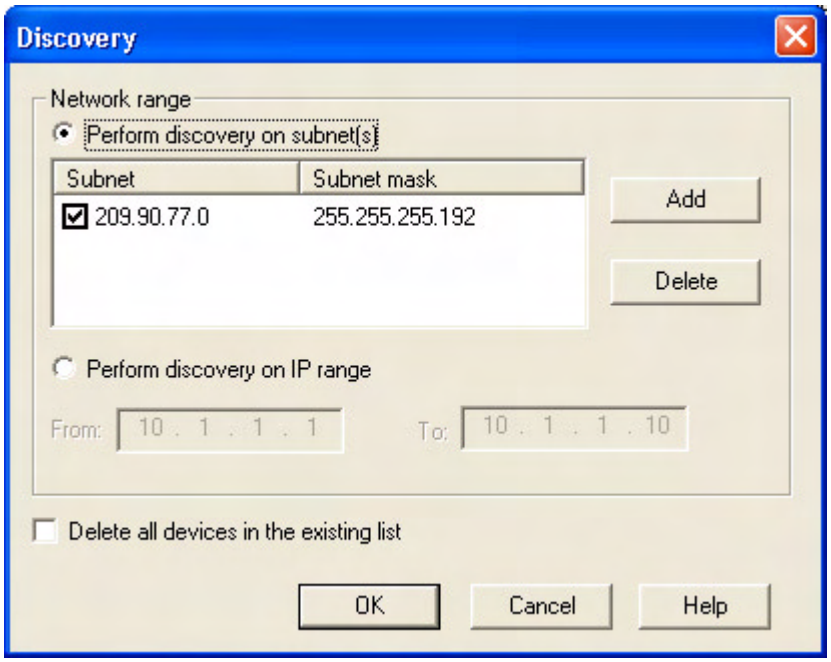
In order to manage the NJ220 IntelliJacks on your network, the Central Configuration Manager needs to include them in its database. The easiest way to add new NJ220 IntelliJacks to the database is to use the device discovery tool included in the Central Configuration Manager.

The first time you run the Central Configuration Manager, it will automatically take you to the Discovery window as shown under step two below. To discover new devices on your network, run the following steps:

1 Open the Central Configuration Manager by double-clicking on the IJ NJ Cent Config Mgr desktop icon. When it launches, you will see a window similar to this one:



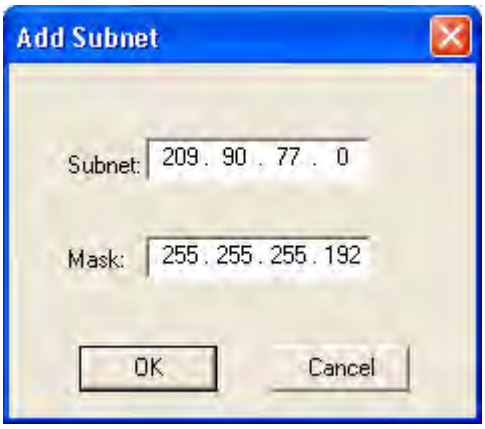
2 Select Discovery from the Devices menu or click the Discover button on the toolbar. The following window will appear:



NOTE: The default subnets are the ones your machine is connected to.

3 You can discover new devices based on a specific subnet or on a specific range of IP addresses.

a To discover devices by subnet, select that option on the screen. Click the Add button to add a new subnet to the discovery list. The following box will appear:



Fill in the Subnet and Mask fields and click OK.

or

b To discover devices within a certain IP range, select that option on the screen and complete the From and To fields.

4 If the box next to "Delete all devices in the existing list" is checked, the discovery process will replace all of the devices in your current database with the new devices it discovers. If unchecked, the discovery process will add newly discovered devices to the current database.

5 Click OK to start the discovery process.

The device discovery tool will return the following information from the NJ220 IntelliJacks on your network:

- IP address
- MAC address
- Subnet address
- Group name
- Location information
- Firmware version

You can sort this information in ascending or descending order.

NOTE: Discovered devices are automatically added to the default database. This default database will open automatically when you launch the Central Configuration Manager. If you like, you can keep several database files, each with its own list of devices. For example, you may want a separate database for each subnet you manage. To save a database file or open another database file, select the Open Database or Save Database As option from the File menu.

You can view discovered devices many ways. On the left side of the toolbar, you can see a drop down box with options for either Subnet, Firmware Ver, or Group Name. The option you select in this box determines how the views are displayed in the left pane of the window.

When Subnet is selected (the default option), you will see a list of IP subnets to choose from. Selecting Network will show all of the discovered devices in the database. If you select a particular subnet, only the devices in that subnet will be displayed.

When Firmware Ver is selected, you will see a list of the different firmware versions loaded on the devices. This view is particularly useful if you want to select only the devices with an old firmware version so you can perform an upgrade.

When you select Group Name from the drop down list, the Central Configuration Manager will present a list of the different group names you have specified.

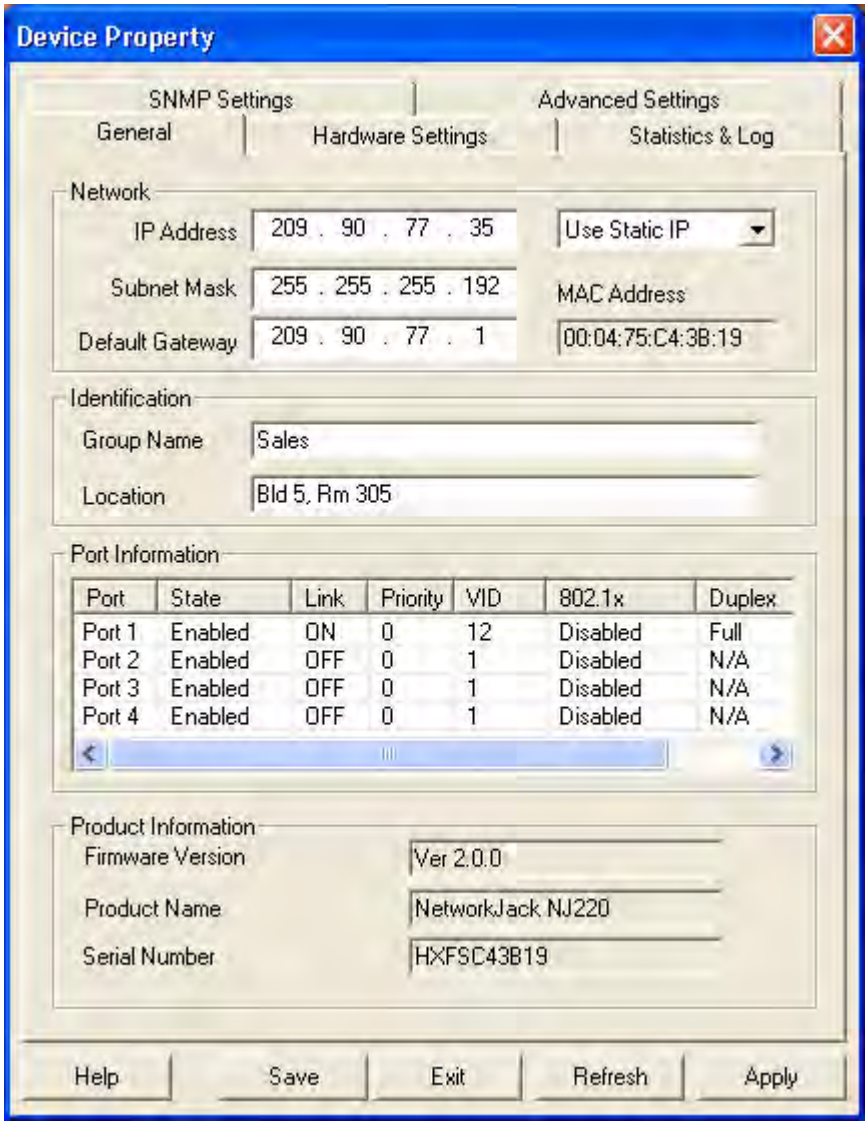
Viewing Device Properties

Once the database is populated with NJ220 IntelliJacks on your network, you can begin to manage those devices. The main window of the Central Configuration Manager shows a list of devices in the current database with the information retrieved during the discovery process. You can view and configure the properties for a **single** NJ220 using this window. To configure multiple devices at one time, see "Changing Device Configuration" on page 43. To get more detailed information about a device, you should check its properties.

The process for configuring one or more IntelliJacks is the same. You choose the changes or configurations you wish to make by selecting them from the various tabs in Device Properties (for changes to a single IntelliJack) or Configure (for single or multiple IntelliJacks). When you have finished making changes, click "Apply" or "OK". You will be asked for your password. The configuration changes will not be made to the IntelliJack until your password has been correctly entered.

1 Select a IntelliJack from the devices list.

2 Select Property from the Devices menu or from the toolbar. You can also open this window by right-clicking your mouse and selecting Property.



General Tab

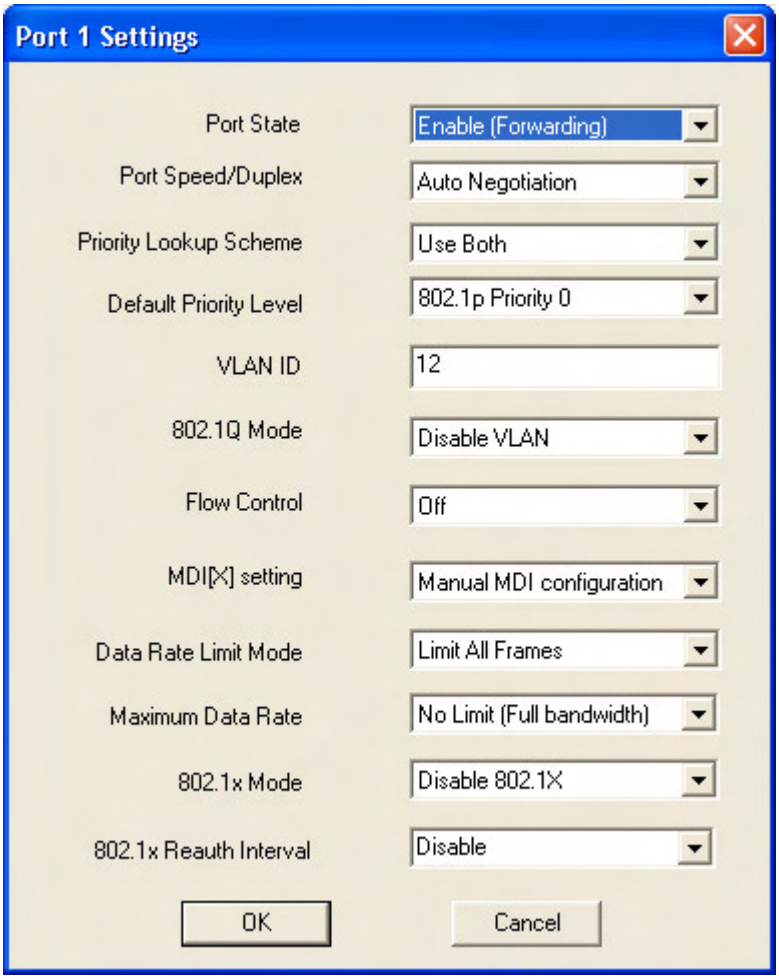
3 With the General tab selected, you can view and edit information about the device such as the IP address, subnet mask, default gateway, and whether it uses a static IP address or gets its address from a DHCP server. You can also view and edit the IntelliJack's Group Name and Location.

4 Click Apply to save any changes you make to the fields in this window.

Port Information

5 In the middle of this window you'll see information about each of the four PAN ports on the front of the IntelliJack. You can check to see if the port is Enabled or Disabled, if there is a network link, its priority, whether or not it's part of a virtual network (VLAN), its 802.1x security setting, if it's running at half or full duplex, and what speed it's set for.

You can double-click on any of the ports to find out more information or configure that particular port.



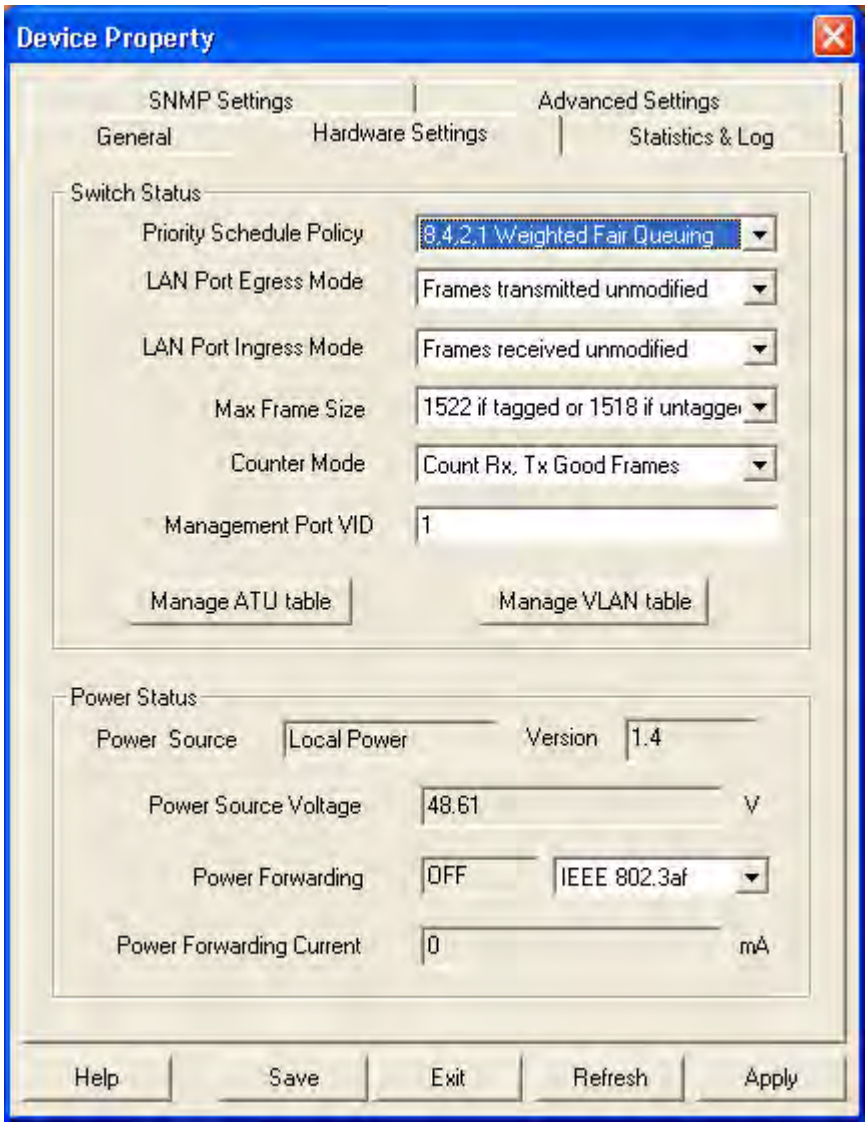
Click OK to save your changes or Cancel to discard them.

Product Information

6 Under the Product Information box, you can see the current firmware version of the IntelliJack, the Product Name, and the Serial Number.

Hardware Settings

7 Click on the Hardware Settings tab to view status information about the switch.



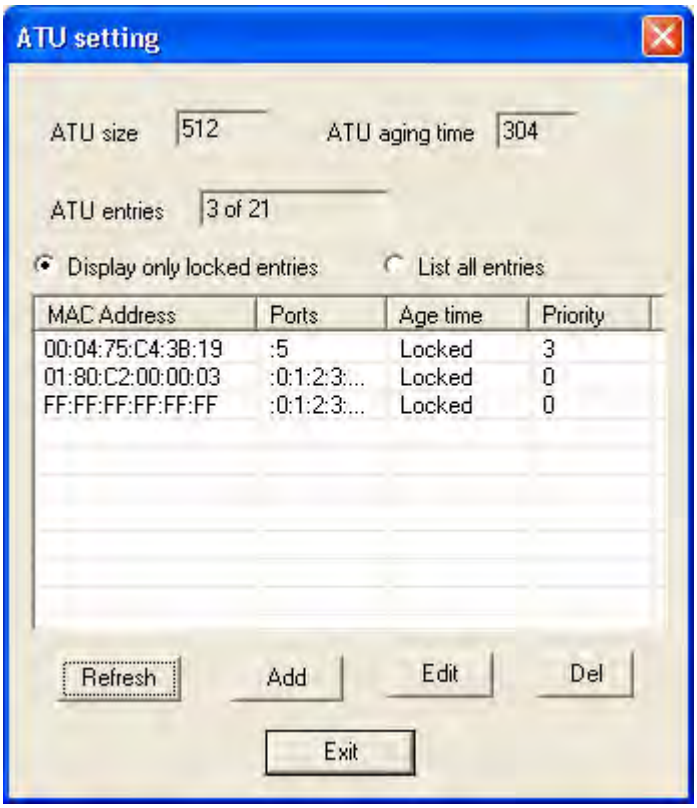
Several fields in this window can be edited, a few cannot. You can change the values of the fields with drop-down lists: Priority Schedule Policy, LAN Port Egress Mode, LAN Port Ingress Mode, Max Frame Size, Counter Mode, and Power Forwarding.

NOTE: For help determining the best configuration options for your system, see the Changing Device Configuration section.

8 Simply select the value you wish to change from the drop-down list of options.

NOTE: You can click Apply at any time to save the changes you have made. But be sure to click Apply after you have finished making all your changes.

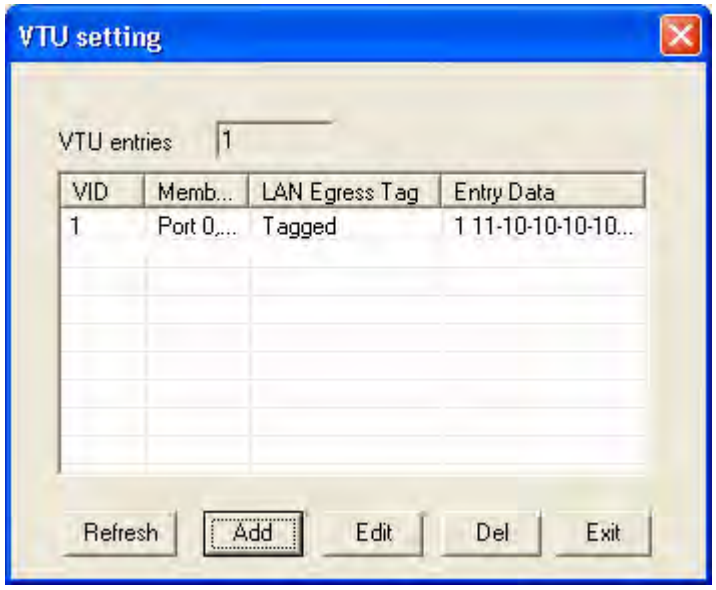
9 Click the ATU Table button to make changes to the NJ220's ATU table. The screen you see allows you to display all MAC addresses that have been plugged into that IntelliJack or just the ones that you have "locked down" to it. You can refresh the list, add MAC addresses to it, edit existing ones or delete entries in the ATU table.



The Address Translation Unit (ATU) performs MAC address searching, learning, and aging functions for all ports of the NJ220 IntelliJack. By default, the ATU table allows a total of 512 entries and an aging time is 304 seconds for each entry.

The NJ220 IntelliJack lets you manage its ATU table. You may want to know which MAC addresses have been plugged into a particular IntelliJack. You may want to associate a MAC address with selected ports, so the unselected ports will not receive frames from this MAC address. You may want to set a certain priority level to the frames associated with the MAC address. Finally, you may want to lock down a MAC address so that it is never dropped from the ATU table. This last operation is referred as MAC address filtering and you can lock down up to 32 MAC addresses into the ATU. All of these configurations are handled through the Properties page, since an ATU table is related to a specific IntelliJack.

10 The NJ220 IntelliJack also lets you manage its VLAN table. To access the VLAN table, click on the Manage VLAN Table button. The screen you see allows you to display all the VIDs that have been assigned to that IntelliJack.

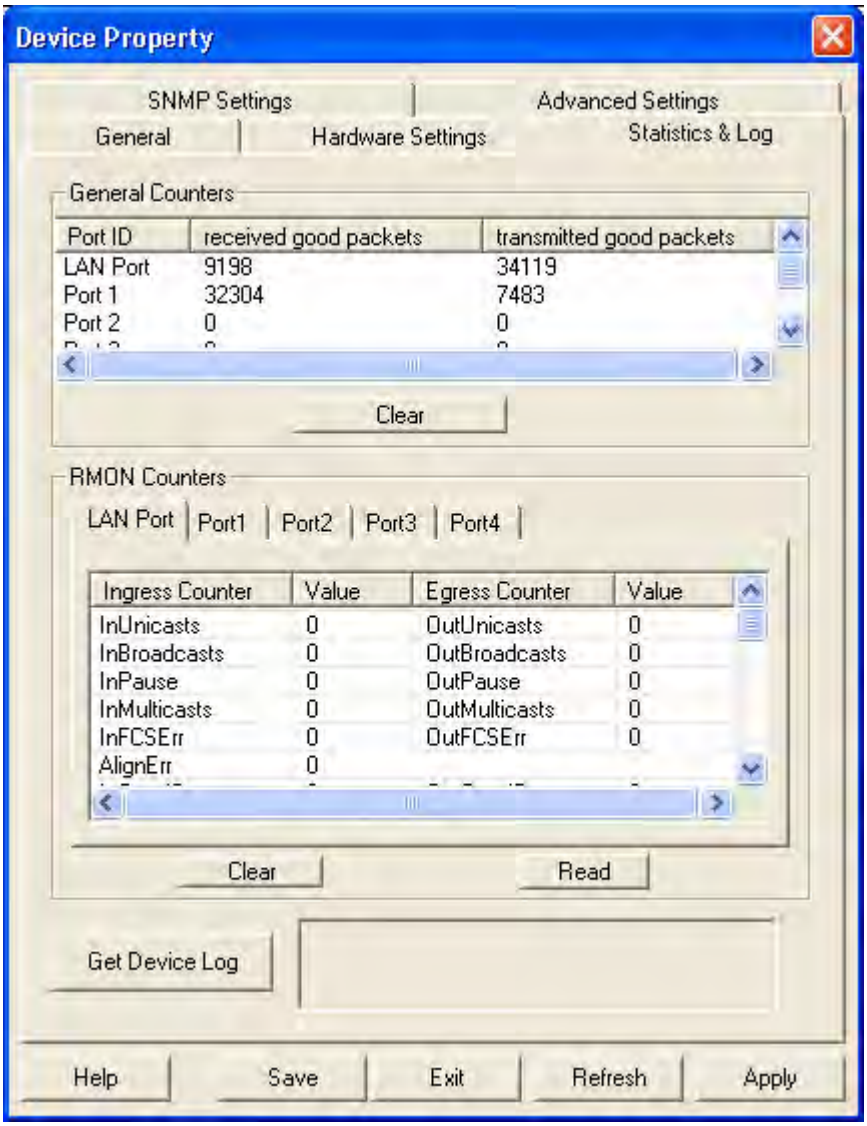


You can refresh the list of VIDs or add to it. You can edit existing VLAN settings, tagging schemes and port associations by clicking the Edit button.

The VLAN table is a record of the VLAN settings which have been configured for a particular IntelliJack. You may want to know which ports have been assigned a VLAN ID (VID), whether packets are tagged or untagged and whether the ports are associated with one another. All of these configurations are handled through the Properties page, since a VLAN table is related to a specific IntelliJack.

Statistics Log

11 Click on the Statistics Log tab.



From this view you can see statistics about the number of good or bad packets each port has received and transmitted, based on how you have configured the Counter Mode setting (see step 7 on page 36).

The bottom half of the window shows Remote MONitoring (RMON) counters for the LAN port and each of the four PAN ports on the IntelliJack. RMON counters are extensions to the Simple Network Management Protocol (SNMP) that provide comprehensive network monitoring capabilities (see appendix C, page 71 for detailed information).

12 To load the counter information from the IntelliJack, click the Read button.

This window lets you monitor the traffic through your network by displaying statistics for many types of packets. The left side shows Ingress counters for packets coming into the IntelliJack's port. The right side shows Egress counters for packets leaving the port.

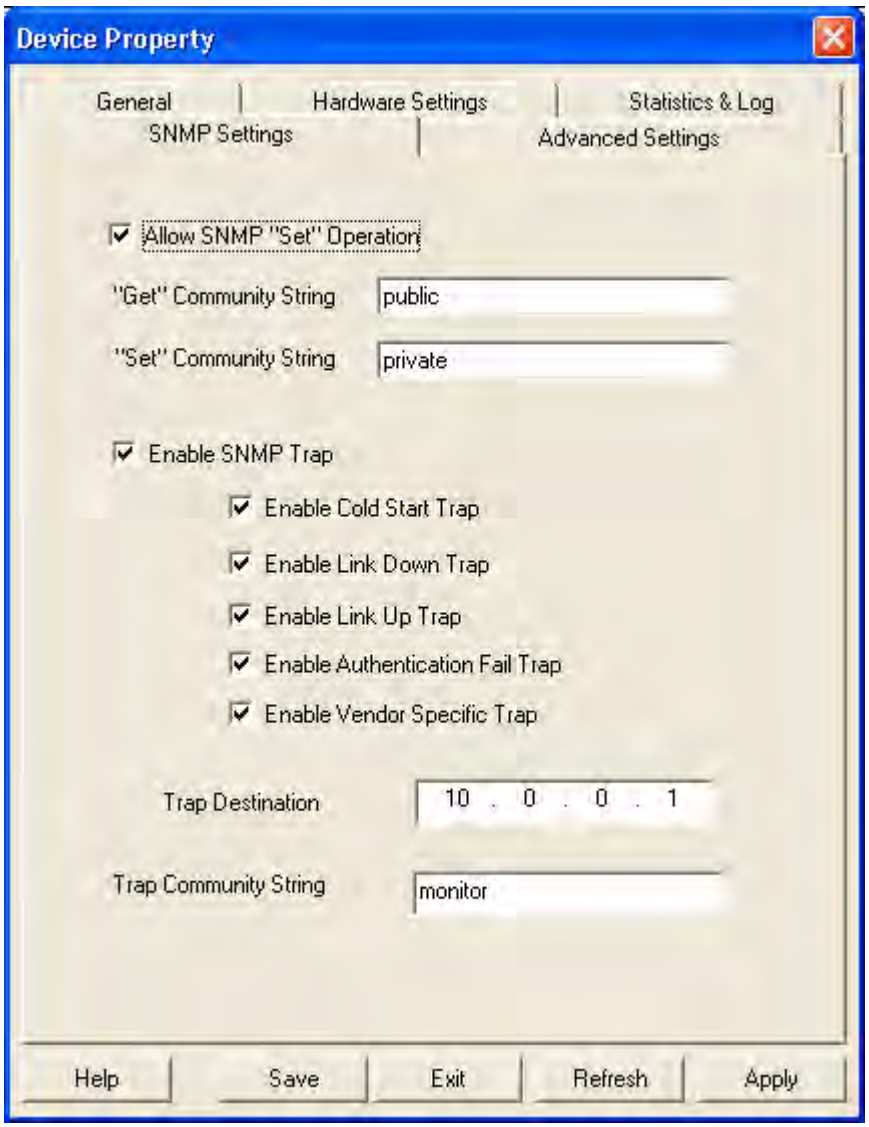
You can reset all counters to zero by clicking Clear.

To save device data to a log file, click Get Device Log. This will prompt you for a filename and location to save the log file.

NOTE: The device log records information regarding watch-dog timer errors or other abnormalities. If, for example, the IntelliJack has unexpectedly rebooted, the event will be recorded in the device log. 3Com Customer Support can use information in the device log to help with troubleshooting. We recommend that you do not attempt to use this log.

SNMP Settings

13 Click on the SNMP Settings tab to see the following window:

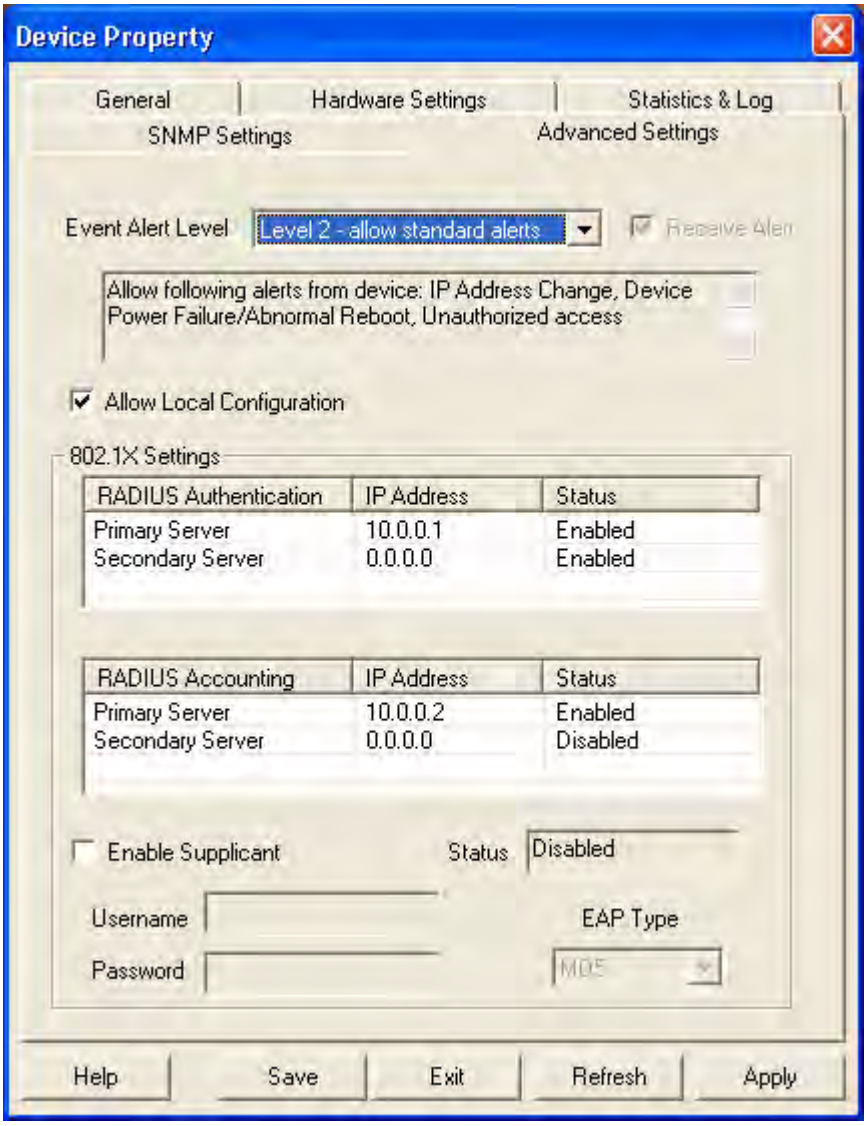


14 You can view and edit the SNMP Community String settings and Trap settings for this particular NJ220.

15 To edit a Trap Destination, enter the IP address of your SNMP management console in the field. This eliminates the need to build a Trap Destination Table via a Management Information Database (MIB) browser.

Advanced Settings

16 Click on the Advanced Settings tab to see the following window:



17 You can view the Event Alert Level and 802.1X Settings configured for this particular NJ220. 802.1X is a security protocol for LANs that relies on the Extensible Authentication Protocol (EAP) to pass messages to RADIUS authentication servers.

NOTE: For help configuring SNMP and 802.1X settings for your system, see the Changing Device Configuration section on page 43.

Different Alert Levels notify you of specific events happening with the IntelliJack. Each level above 0 provides different types of event alerts as described below:

Alert Level	Notifying Event
Level 0: Disable all alert messages	None
Level 1: Allow critical alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
Level 2: Allow standard alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
	Unauthorized Access
Level 3: Allow all alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
	Unauthorized Access
	Normal Reboot
	NBX phone plugged in
	NBX phone removed

Next to the Event Alert Level field is a box labeled Receive Alert. If you are running the Central Configuration Manager on more than one machine in your organization, the Receive Alert box will only be active for the last CCM that discovered the device. The box will be grayed out on the CCMs of all other machines.

18. Click Apply to save any changes you make, and a configuration summary dialog box will appear. Verify the information and click OK.
19. Click Exit to close the Device Property window.

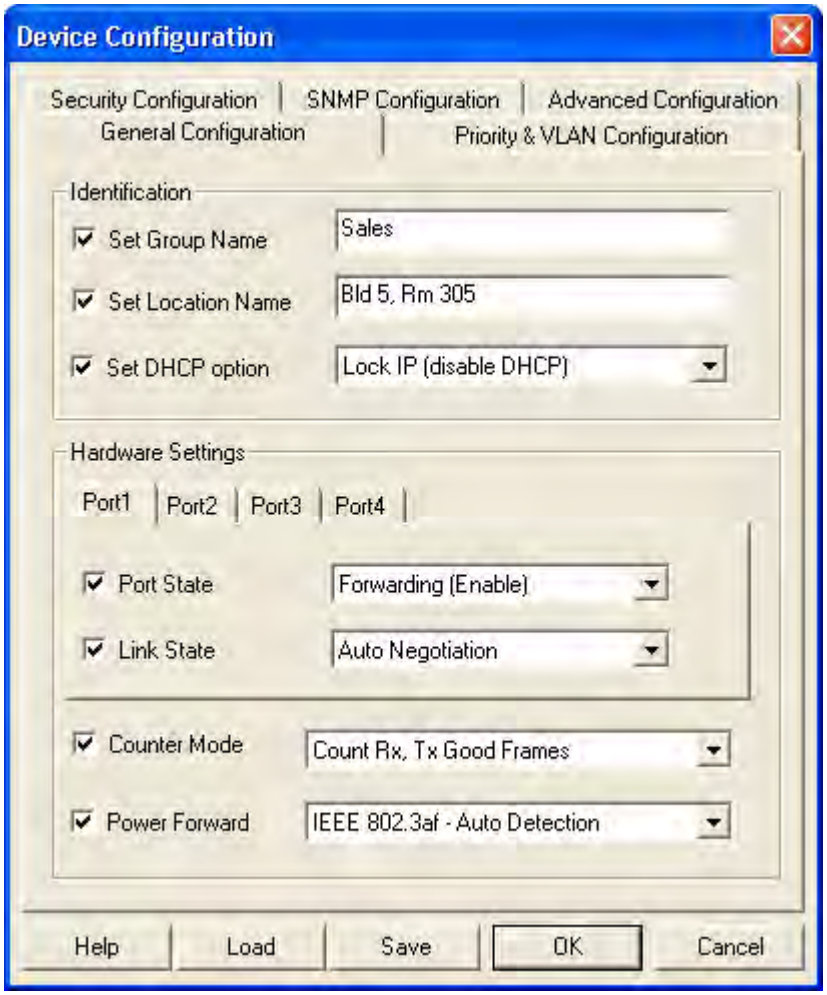
Changing Device Configuration

Many of the properties that you can view from the Device Property windows can be changed from the Device Configuration window. Here's how to use this feature:

1 Select one or more IntelliJacks from the devices list.

NOTE: It is possible to configure multiple IntelliJacks at the same time.

2 Select Configuration from the Devices menu or the toolbar, or right click on a device and select Configuration from the pop-up menu.



NOTE: To make configuration changes to a IntelliJack from the Central Configuration Manager, the NJ220 must be part of the device database. See the section on Discovering NJ220 Devices on Your Network for information about including new devices in the database.

You must also be able to communicate with the device from your workstation in order to configure it. If you can't communicate with the device at this time, you will receive an error message.

This window has five tabs across the top--General Configuration, Priority & VLAN Configuration, Security Configuration, SNMP Configuration, and Advanced Configuration. Check the box next to any setting you want to change from within these five areas.

The bottom of the window has buttons labeled Load and Save. The Save operation lets you save an IntelliJack configuration profile. You can then use the Load button to apply the configuration profile to one or more IntelliJacks.

If you wanted to send a single configuration to one or more IntelliJacks, you would make the configuration changes in this window and click Save. Then you could select a list of IntelliJacks from the main Configuration Manager window and click Load, choose the file, and click Okay. This would send the configuration to all of the IntelliJacks that you selected.

General Configuration

3 Make sure the General Configuration tab is selected.

Identification Settings

4 To change or set the Group Name, check the box next to that field. You can set a Group Name to anything you want, up to 128 characters.

5 Change or set the Location Name by checking the box next to that field and entering up to 128 characters.

6 Configure the DHCP setting to the desired state.

Hardware Settings

7 Change the Port state of any of the IntelliJack's ports by selecting the Port tab and checking the box next to the characteristic you want to modify. Then select a value from the drop list.

Forwarding (Enable) is the default setting for the Port State. The other option is Blocking (Disable). Forwarding (Enable) allows traffic to pass through the individual ports. By setting the Port State to Blocking (Disable), you can block any traffic from passing.

You may want to set the Port State to Blocking (Disable) when you want to restrict access to your LAN at the location where the IntelliJack is installed. This might be an appropriate option in a public use area such as a lobby, conference room, or classroom. Using the Calendar function, you can schedule the Port State for Forwarding (Enable) or Blocking (Disable) at specified times and dates.

8 To change the Link State setting, click the box and select an option from the drop list.

Auto Negotiation is the default setting and the de facto setting for most network equipment because it is the most flexible option. It automatically configures a networked device based on the speed and duplex of the upstream device it is plugged into. This is especially useful when you do not know the configuration (speed/duplex) of all devices connected to the network.

Be advised, however, that not all network interface cards (NICs) use the standard auto-negotiation algorithm, and it may be necessary to force the speed and duplex of the PAN port to match the speed and duplex of the attached NIC.

9 The next two settings apply not to a specific port, but to the IntelliJack as a whole. By default, the Central Configuration Manager will display a count of good

transmissions in the Property window because it is unlikely that the IntelliJack will drop any Ethernet Packets.

If you believe that the IntelliJack is dropping Ethernet packets, you may want to configure the Counter Mode to count received errors (Rx Errors) and transmission collisions (Tx Collisions). This will give you a good sense of whether packets are actually being dropped.

10 To change the Power Forwarding setting, click the box and select an option from the drop list.

IEEE 802.3af is the recognized standard for Power over Ethernet (POE) and the default setting. More and more network devices that are POE capable are adhering to this standard.

The IntelliJack's Power over Ethernet capability also lets you forward power to a standards-compliant device plugged into Port 1 of the NJ220. The default setting of the NJ220 is auto-detect. We recommend that you keep this setting as part of your configuration to ensure that power will only be forwarded to devices capable of receiving it.

The IEEE802.3af standard requires a powered device to present a signature to the power sourcing equipment. The power sourcing equipment will check this signature and will only apply power to the line when it sees the correct signature.

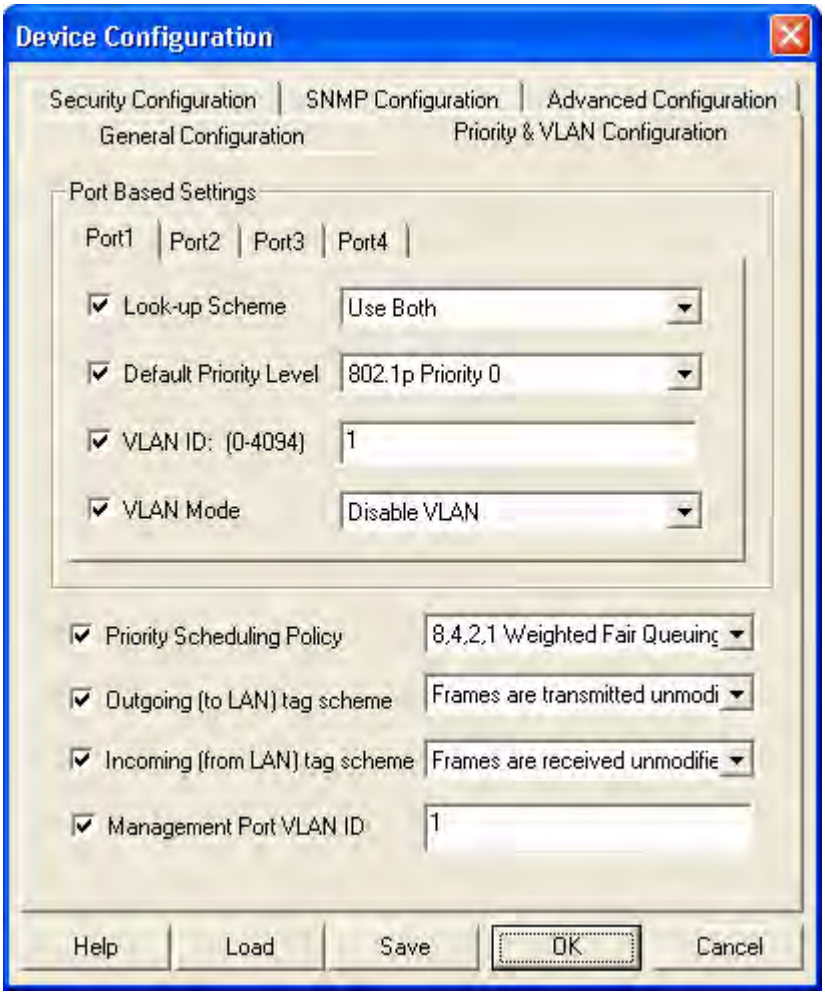
If you want to ensure that power will not be forwarded at all, however, you could select Force power OFF to any device connected to Port 1.

Select Force power ON if you always want to apply power to any device plugged into Port 1. This option would let you power devices plugged into Port 1 that do not have the signature required by IEEE802.3af-compliant power sourcing equipment.

WARNING: By forcing power ON, you may damage equipment that is inadvertently plugged into Port 1, such as a device that is not designed to handle 48V.

Priority & VLAN Configuration

11 Click the Priority & VLAN Configuration tab along the top of the Device Configuration window to view these settings:



Port Based Settings

12 To change the Port Based Settings, first select the Port's tab you want to make the changes to.

13 To change the Look-up Scheme from the default of Use Both, click the box and select an option from the drop list.

Both the Use IEEE 802.1p Traffic Class Field and Use IP TOS, DiffServ fields look-up schemes examine Ethernet packets to determine their prioritization. The former looks at one portion of the packet, effectively making it a Layer 2 tool. The latter looks at a different part of the packet, effectively making it a Layer 3 tool.

The Look-up Scheme is part of the prioritization of Ethernet packets. Prioritization determines which packets clear the buffer first. If you didn't care about the prioritization of packets, you would choose None. If you wanted to prioritize voice packets on Port 1, for example, you would choose another option.

14 The default setting for the Default Priority Level is 802.1p Priority 0 or 1. You can change this setting to Priority 2 or 3, Priority 4 or 5, or Priority 6 or 7.

The IntelliJack has four traffic queues with two priorities per queue. The lowest numbers (0 and 1) have the lowest priority. The default priority traffic is called "Best Effort" and serves as a baseline priority for all standard Ethernet traffic.

If you want to assign a higher priority to traffic on a particular port (voice traffic, for instance), you can do so. The higher the number the higher the priority (Priority 6 or 7 is the highest). The IntelliJack will send higher priority traffic ahead of lower priority traffic to improve the quality and throughput from that particular port.

15 You can associate any of the four ports with any other ports on this IntelliJack to form a VLAN group. You can specify the tag schemes for the VLAN you create.

You can set the VLAN ID (VID) field to any number between 0 and 4094. The default setting is 1, which is the common practice. If all equipment is set at VID 1, you can communicate across all ports.

Since VLANs are used to separate network traffic to make it more manageable and secure, you would change the VID of the individual ports to meet the needs of your network.

In a classroom setting, for example, you may want the teacher to be on a separate VLAN than the students. You could assign VID 10 to Port 1 of the IntelliJack for the teacher and VID 20 to the other ports.

NOTE: The VID of a port must match the upstream switch VLAN assignments. If the IntelliJack's VID assignments do not match the upstream switch and "add a VLAN tag" is set in the Egress rule, then the traffic that passes from the IntelliJack to the LAN will be dropped at the upstream switch port.

16 To change the VLAN mode setting, click the box and select an option from the drop list. You can choose to Disable the VLAN. In this mode, ingress frames are forwarded through default switching rules.

You can also choose Enable unrestricted VLAN. In this mode, the port is associated with the current VLAN ID you have set. Frames ingressed into this port without a VLAN tag or with the same VLAN ID are forwarded within the VLAN. Frames with a different VLAN ID are forwarded according to default switching rules (i.e., based on the destination MAC address). Management packets are able to pass through this port on this setting.

Finally, you can choose Enable restricted VLAN. In this mode, the port is associated with the current VLAN ID you have set. All frames ingressed into this port are forwarded within the same VLAN, and management packets are blocked on this port.

Other Priority & VLAN Settings

17 Click the box and select from the drop list to change the Priority Schedule Policy. The default setting is 8,4,2,1 weighted fair queuing scheme.

8,4,2,1 refers to the number of bytes removed from the IntelliJack's buffer. 8 bytes of the highest priority traffic are removed from the buffer first, then 4 bytes from the second most important, 2 bytes from the third, etc. This is the most common priority scheme because it ensures that important traffic is prioritized but still allows traffic flow for all ports.

In a strict priority scheme (the setting's other option), all highest priority traffic will be removed from the buffer. After it is removed, the next priority traffic type would be removed, and so on. This ensures that the most important or time critical data is passed first, but it could potentially slow traffic from other ports.

18 You can change the Outgoing (to LAN) tag scheme for the IntelliJack. By default, frames are transmitted unmodified. This setting ensures that you will not risk losing communication with upstream switches due to misaligned VLAN IDs (VIDs).

If you want to configure traffic from a port on the IntelliJack, you can add a tag to the frame. This lets you separate traffic into different VLANs.

19 You can also change the Incoming (from LAN) tag scheme. By default, all frames are received unmodified. By receiving frames unmodified, you will not risk losing communication between upstream switches and the devices connected to the IntelliJack due to misaligned VIDs.

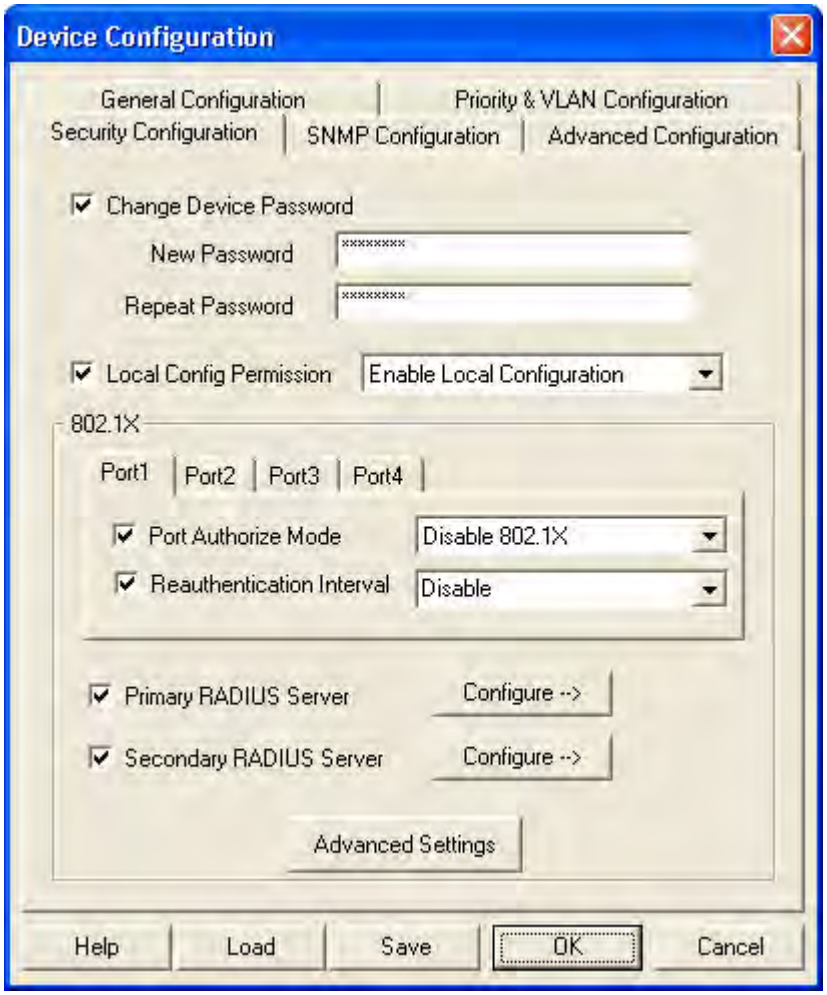
If an upstream switch is sending a tagged packet but the device connected to one of the IntelliJack ports does not need the tag information, you can remove the tag.

20 It is common practice to set the VLAN ID (VID) of the management port to VID 1, and this is the default value.

The management port is the port through which all commands to and from the IntelliJack are communicated. You may want to separate management traffic from other network traffic by assigning the Management Port of the IntelliJack to a different VID. You should make sure that the VID for the management port of the IntelliJack is the same as the VID for management ports of upstream devices.

Security Configuration

21 Select the Security Configuration tab to set the security options of the NJ220 IntelliJack.



Password

22 You can change the device password (the default password is "**password**"), and either enable or disable local configuration.

NOTE: You should change the password to ensure that no one else can re-configure your system. Make sure you remember the new password you set. ***If you forget the new password, you will not be able to perform any other configuration tasks unless you send the device back to 3Com****.*

802.1X

23 To change 802.1X settings for a specific port, select that port's tab and make the changes by clicking the box and selecting an option from the drop list. The default setting for Port Authorize Mode is Disable 802.1X.

802.1X is a standard for port-based network access control. Typical 802.1X implementations in an Ethernet switch usually include the authenticator as well as

RADIUS clients. The authenticator controls port access for the network client devices connected to the switch.

When the option is set to Disable 802.1X, all packets are processed as a normal Ethernet switch; no 802.1X control applies.

With Standard 802.1X selected, control is enabled. Once the device is authorized, the port it connects to is in the authorized state and all packets entering the port are allowed to pass through.

When the Secure 802.1X option is selected, control is enabled. In addition, the IntelliJack will check its ATU to determine if packets entering the port should be forwarded. If the device is authorized, the IntelliJack will put the MAC address of the device in the ATU and allow its packets to pass through. The NJ220 will block all other packets that don't have the correct MAC address specified in the ATU.

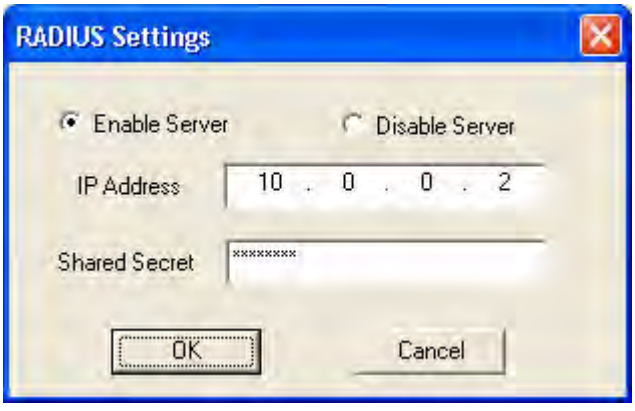
You can select the MAC address filter option if a client device does not support 802.1X and wishes to connect to the network through the IntelliJack (e.g., a network printer). In this case, you can manually add the device's MAC address associated to the port in the ATU, and packets from the network to this port will be blocked unless their MAC addresses are listed in the ATU.

802.1X with IP Phone is a special case of 802.1X secure mode. In this mode, when a 3Com IP phone is connected to the IntelliJack, the phone's MAC address will be locked into the ATU automatically. Therefore, packets sent from the phone can pass through by default without further authentication. If 802.1X control is not required, an IP phone can connect to a port with 802.1X disabled and voice traffic will pass through without authentication.

24 When 802.1X security is applied, authentication is required and reauthentication is required at specific intervals. The IntelliJack disables reauthentication by default.

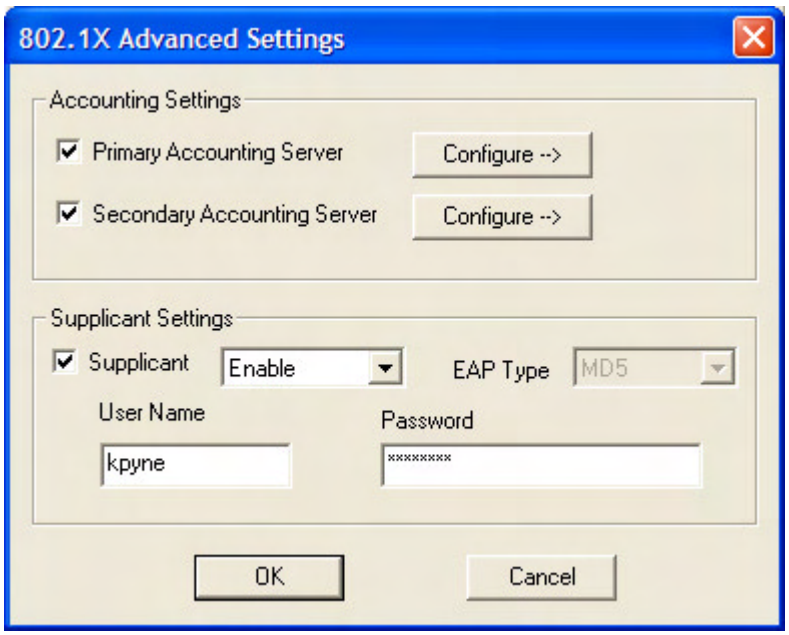
When reauthentication is enabled, the default period is 3600 seconds. You could select an interval ranging from 10 to 65535 seconds. If you prefer that a supplicant device authenticates itself on a frequent basis, you would choose a small reauthentication interval. Likewise, you would increase the interval or disable the function if you were not concerned about regular authentication of the devices on your network.

25 To use 802.1X, you must select a RADIUS server to act as authenticator to devices connected to the NJ220. To select a Primary or Secondary RADIUS server, click the box and the Configure button. This will open a separate window.



In this box you can Enable or Disable the server, enter the server's IP address and the Shared Secret.

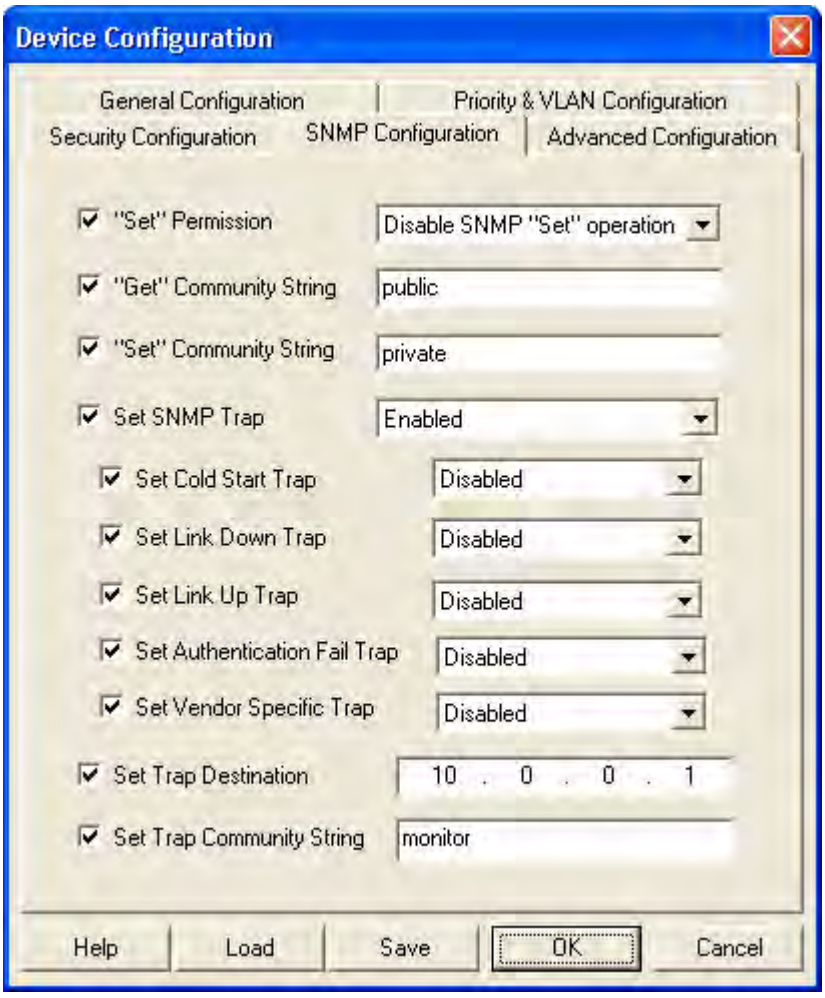
26 To set advanced 802.1X security settings, click the Advanced Settings button in the Security Configuration window.



Primary and secondary accounting servers are similar to the settings for RADIUS servers. The supplicant settings let you configure the IntelliJack as a supplicant to an 802.1X-enabled upstream switch. To enable this option, select the box next to Supplicant. When you do, the other fields on the screen will become active. You can enter a Supplicant User Name and Password as well as an EAP Type setting. MD5 is the only EAP type that the IntelliJack currently supports.

SNMP Configuration

27 Click the SNMP Configuration tab to change the SNMP settings of the NJ220.



28 You can either Enable or Disable the "Set" operation of the IntelliJack.

29 Configure the "Get" and "Set" Community Strings for SNMP management operations.

30 Enable or Disable SNMP Trap with the Set SNMP Trap setting. Once enabled, you have the ability to configure the remaining trap settings.

SNMP provides the ability to send traps (notifications) to a trap destination, such as an SNMP server, when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. When the condition for the trap has been met, the SNMP agent forms an SNMP packet and sends it to the administration application.

- A Cold Start Trap signals the administration application when the IntelliJack does a Cold Start.
- A Link Down Trap signals when the SNMP agent on the IntelliJack has gone to "down" state and is not reachable.
- The Link Up Trap signals when then SNMP agent has gone to the "up" state and is now reachable.

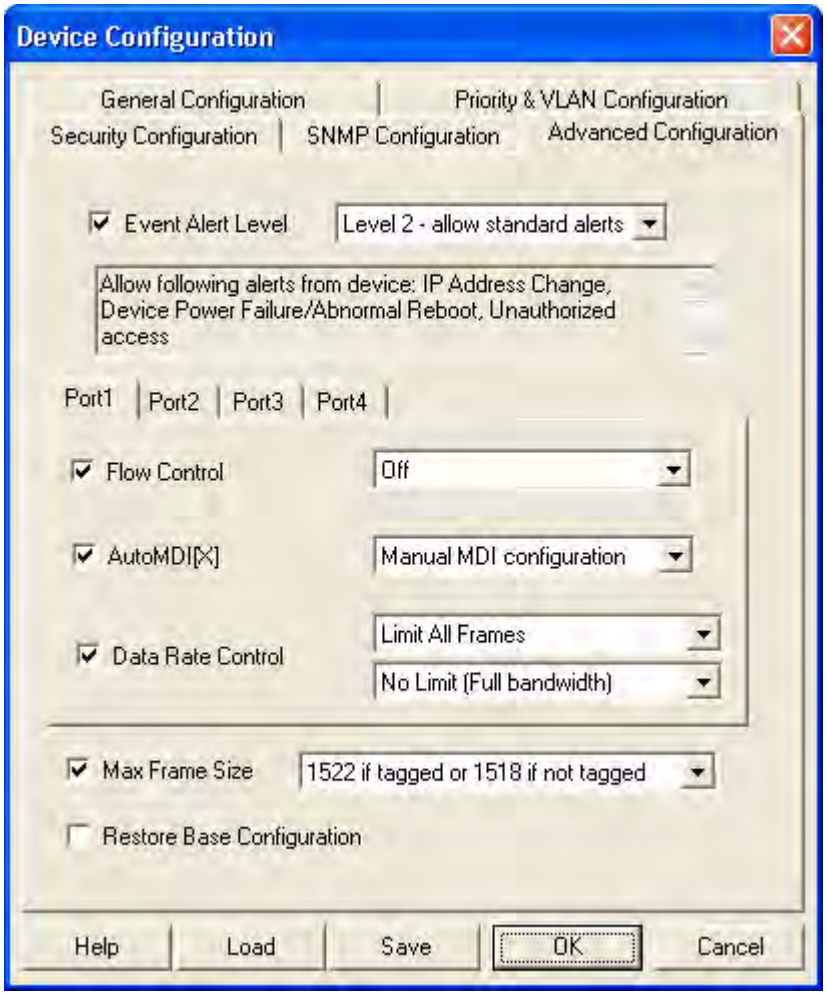
- An Auth Fail Trap indicates a wrong Community name in the SNMP transmission.
- Vendor Specific Traps indicate 802.1X User Login, 802.1X User Logout, and 802.1X Login Failure when the IntelliJack is configured for 802.1X.

31 You can Set Trap Destination by entering the IP address of your SNMP management console. This eliminates the need to build a Trap Destination Table via a Management Information Database (MIB) browser.

32 Set the Trap Community String in the final field of this window.

Advanced Configuration

33 Select the Advanced Configuration tab for this window:



Event Alert Levels

34 At the top of this window is a setting to specify the Event Alert Level. The NJ220 can alert you when specific events occur. While this lets you monitor and respond to network events more quickly, it also creates an additional workload. As a result, the default setting is "disable all event notification" with additional levels of alerts depending on how many events you want to monitor.

You can change the Alert Level if you want to be notified of specific events happening with the IntelliJack. Each level above 0 provides different types of event alerts as described below:

Alert Level	Notifying Event
Level 0: Disable all alert messages	None
Level 1: Allow critical alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
Level 2: Allow standard alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
	Unauthorized Access
Level 3: Allow all alerts	Device Power Failure/Reboot
	Abnormal Reboot
	IP Address Change
	Unauthorized Access
	Normal Reboot
	NBX phone plugged in
	NBX phone removed

Port Based Controls

35 For the next three settings, first select the port you want to configure.

36 You can turn on Flow Control for a specific port. Setting Flow Control to Off (the default setting) allows full passage of traffic regardless of how quickly it is processed by the IntelliJack.

You may want to turn Flow Control On if you discover that large amounts of traffic are being sent to the IntelliJack and it is dropping Ethernet packets. The Flow Control sends a message to the upstream switch the IntelliJack is connected to, telling it to slow down the rate at which it forwards traffic. This will slow down the network.

37 The IntelliJack has the ability to configure AutoMDI[X]. Manual MDI configuration (the default value) assumes that the patch cords between the IntelliJack's PAN port and the device it's plugged into are straight-through cables (not cross-over cables).

If you use cross-over cables to connect devices to your network, you would need to set this option to Manual MDIX Configuration so that network traffic can pass between the device and the PAN port of the IntelliJack.

38 You may want change the Data Rate Control options. The default settings allow all types of traffic to pass through the IntelliJack at full bandwidth.

You can change the frame limitations to slow down or block particular types of traffic. For example, you may want to allow unicast traffic to pass at full bandwidth but restrict broadcast traffic because you are concerned about a type of virus that triggers broadcast storms. With the Data Rate Control, you can configure the IntelliJack to only allow unicast traffic to pass.

With Data Rate Control settings, you can reduce the network traffic speed on the IntelliJack to as little as 128 Kbps. This can be useful if the machine is in a public area where you only want to provide a minimum speed connection.

Even though there are only eight rate limiting choices in the pull-down menu, you can actually increase the number of options you have by setting the Priority Levels on the Priority and VLAN Configuration tab. The following chart shows the various options you can choose on a per port basis:

Priority Option	**0**	**2**	**4**	**6**
Multiplier	1	2	4	8
Rate limiting option				
128 Kbps	128 Kbps	256 Kbps	512 Kbps	1 Mb
256 Kbps	256 Kbps	512 Kbps	1 Mb	2 Mb
512 Kbps	512 Kbps	1 Mb	2 Mb	4 Mb
1 Mb	1 Mb	2 Mb	4 Mb	8 Mb
2 Mb	2 Mb	4 Mb	8 Mb	16 Mb
4 Mb	4 Mb	8 Mb	16 Mb	32 Mb
8 Mb	8 Mb	16 Mb	32 Mb	64 Mb
No limit	Up to 100 Mb	Up to 100 Mb	Up to 100 Mb	Up to 100 Mb

39 You can change the Maximum Frame Size setting if your network uses non-standard frame sizes.

The standard maximum size of an Ethernet frame is 1518 bytes. If a VLAN tag is added, the maximum size increases to 1522 bytes. As a result, this is the default setting. If your network uses larger frames, you can select the 1535 byte option.

Restoring Default Values

40 At the bottom of this window is an option to restore some of the configuration settings to their default values. If you check this box, the following settings will be restored:

Global Setting	**Default Value**
Max Frame Size	1518 or 1522 if tagged
Counter Mode	Count good frames
Priority Scheduling Mode	8, 4, 2, 1 weighted
VLAN Tag for LAN Port (egress)	Egress frame unmodified
VLAN Tag for LAN Port (ingress)	Ingress frame unmodified
Power Forward	Auto detection
Local Configuration	Enable
SNMP SET	Enable
SNMP Traps	Disabled
Event Alert	Level 2
ATU Table	Blank
VTU Table	Blank
All RADIUS settings	Blank

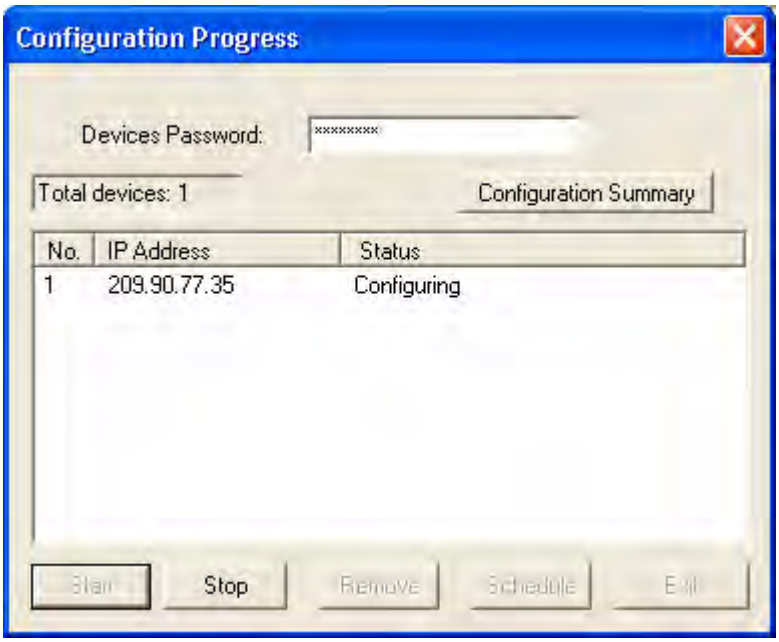
Global Setting	Default Value
802.1X Supplicant Status	Disabled
802.1X Supplicant User Name and Password	Blank

Port Setting	Default Value
State	Forwarding
Link	Auto negotiation
Flow Control	Off
MDI[X]	Force MDI
Multicast Limit	3%
Priority Lookup	Tag & IPV4
Port Priority	0 or 1
VLAN ID	1
802.1Q VLAN Mode	Disable VLANs
Data Rate Limit	All frames
Maximum Data Rate	No limit

The values that remain unchanged when you click Restore Base Configuration are:

- Group Name
- Location Name
- Password
- IP Address
- DHCP Settings
- SNMP Get, Set, and Trap Community Strings
- SNMP Trap Destination IP Address
- Subnet Mask
- Gateway
- Device Log (stored in EEPROM)
- Management Port VID

41 When you are finished entering the configuration changes to your NJ220 IntelliJack, click the OK button and a Configuration Progress dialog box will appear. If you don't want to apply the changes you made, click Exit to discard those changes and exit the window.



42 If you click Configuration Summary, you will see a summary of all the changes you have made. Enter your password and click Start. As the IntelliJacks are configured, their status will be updated in the Status column.

43 If you want to schedule the configuration changes to take effect at a later time or date, click the Schedule button. The schedule function lets you schedule when you want a configuration operation to occur. For example, you could turn ports on and off at pre-designated times. In a public area, for instance, you may want to provide network access between the hours of 7:00 a.m. and 10:00 p.m. You can use the schedule function to automatically turn off the ports at 10:00 p.m. You can even use this feature to automatically repeat the operation on a regular basis.

NOTE: If a NJ220 IntelliJack that was once discovered by the Central Configuration Manager is no longer connected to your network or if you just want to remove a device from the current database, you can select Delete Device from the Devices menu.

From the file menu, you can use the features Backup and Restore. The Backup operation lets you save a snapshot of the configuration of one or more IntelliJacks. You would most likely use the Backup operation if you wanted to save the configurations of a number of IntelliJacks (e.g., all the IntelliJacks in a particular subnet).

When you use the Backup operation, you will be asked for a Secret Key. This is different than the IntelliJack passwords you have already defined. It is a password that protects the backup configuration.

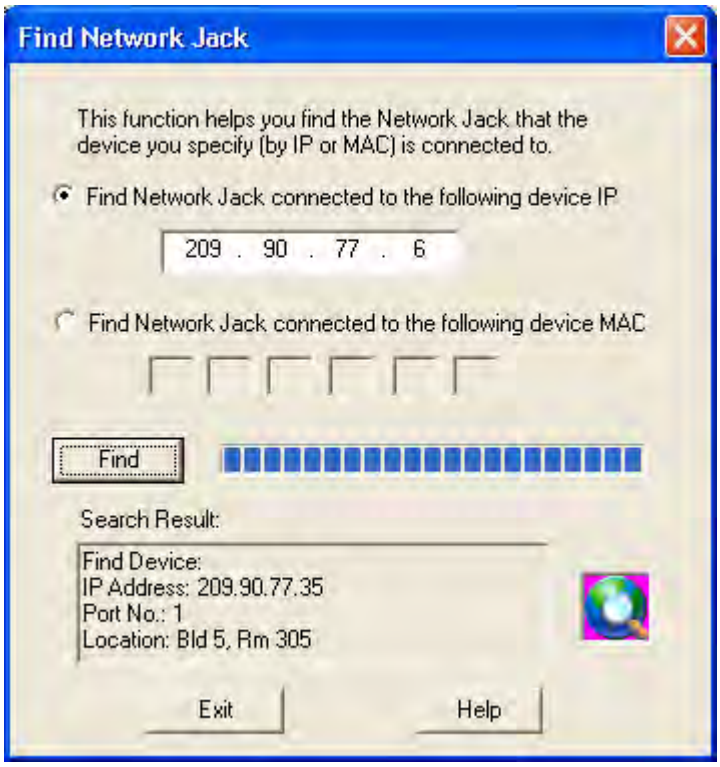
The Restore operation lets you recover configurations you saved with Backup. When you initiate a Restore, you will be asked for the Secret Key you established with the Backup operation.

Finding Computers Connected to NJ220 Devices

Occasionally you may need to find out which IntelliJack a networked device, such as a PC, is connected to. This is one of the many situations where the Location Information field of the NJ220 can be very useful.

If you know the IP address or MAC address of the computer or networked device, you can use the Central Configuration Manager to find the right IntelliJack.

1 Select Find Location from the Tools menu. You will see a window like this:



2 Enter the IP address or the MAC address of the network device you wish to find.

3 Click the Find button.

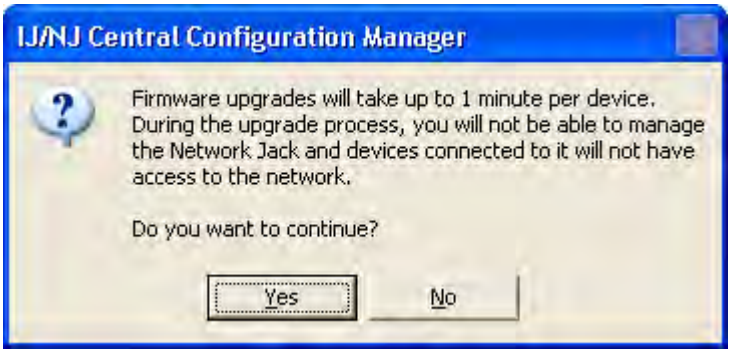
When the search is complete, the Search Results field will display the IP address of the NJ220 that the network device is connected to. It will also show the Location Name assigned to the IntelliJack and which PAN port the network device is using.

4 Click OK to close the window.

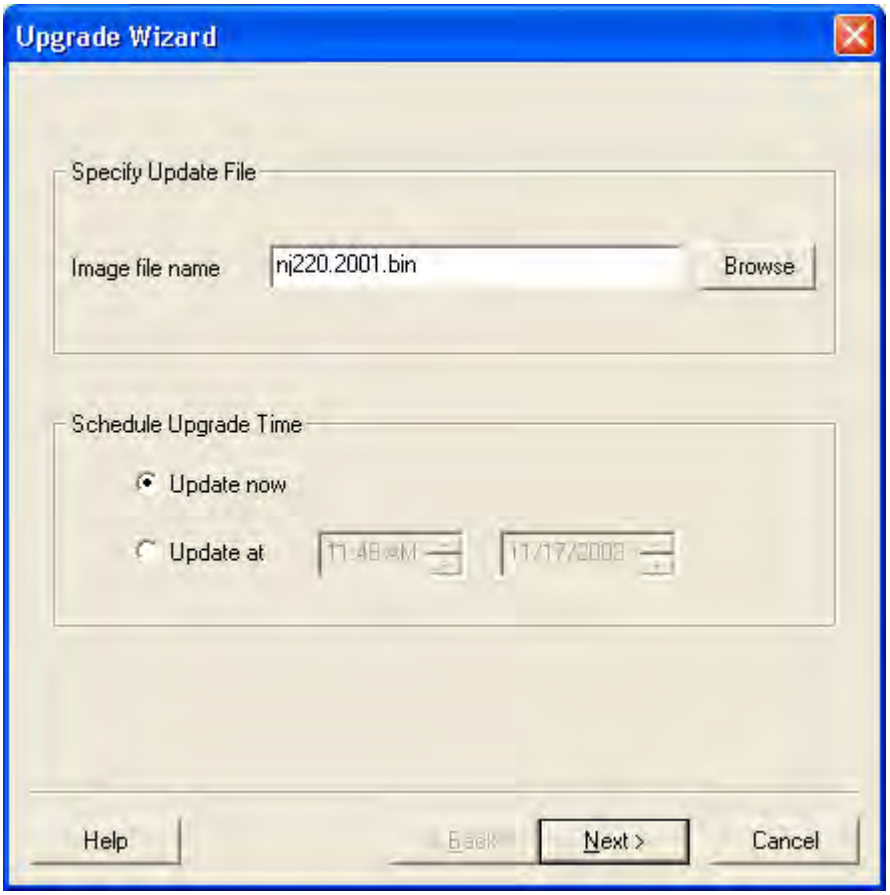
Upgrading the NJ220 Firmware

You can upgrade the firmware on your NJ220s over the network from the Central Configuration Manager. To do so, follow these steps:

1. Select one or more IntelliJacks you want to upgrade. You can select groups of IntelliJacks using one of the grouping options available to you in the drop-down list at the top left corner of the main window.
2. Select Upgrade from the devices menu. A window like this will appear:



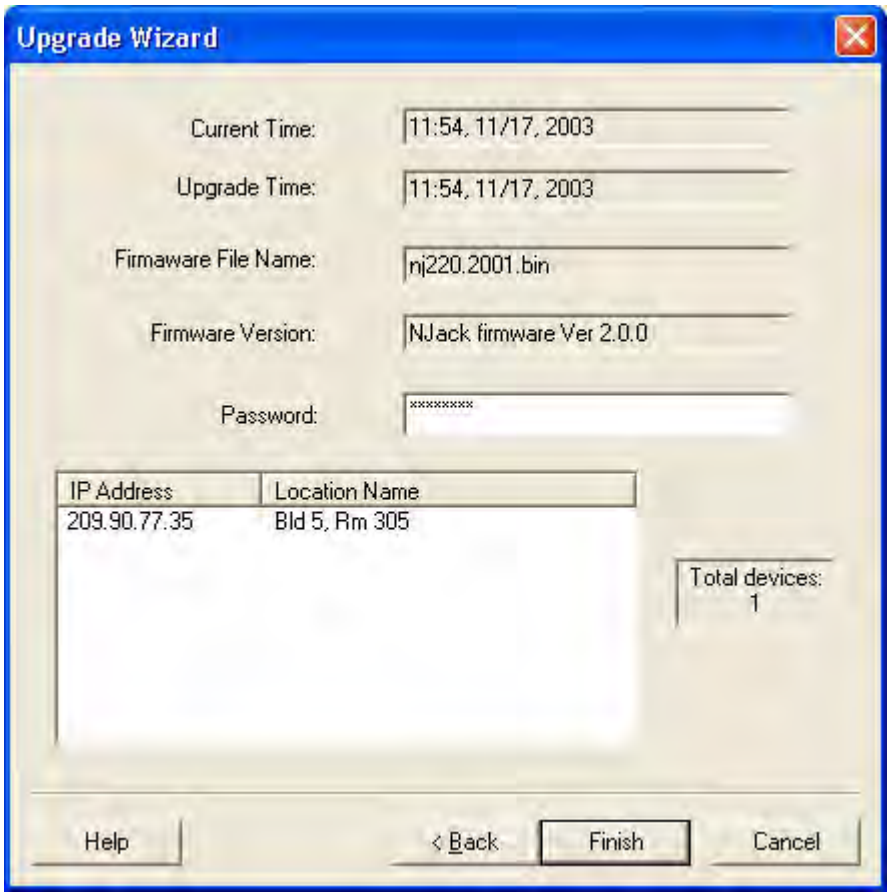
3. Select Yes to continue the upgrade operation. A window like this will appear:



4. Select a valid firmware image by typing the path to the file or by using the Browse button.

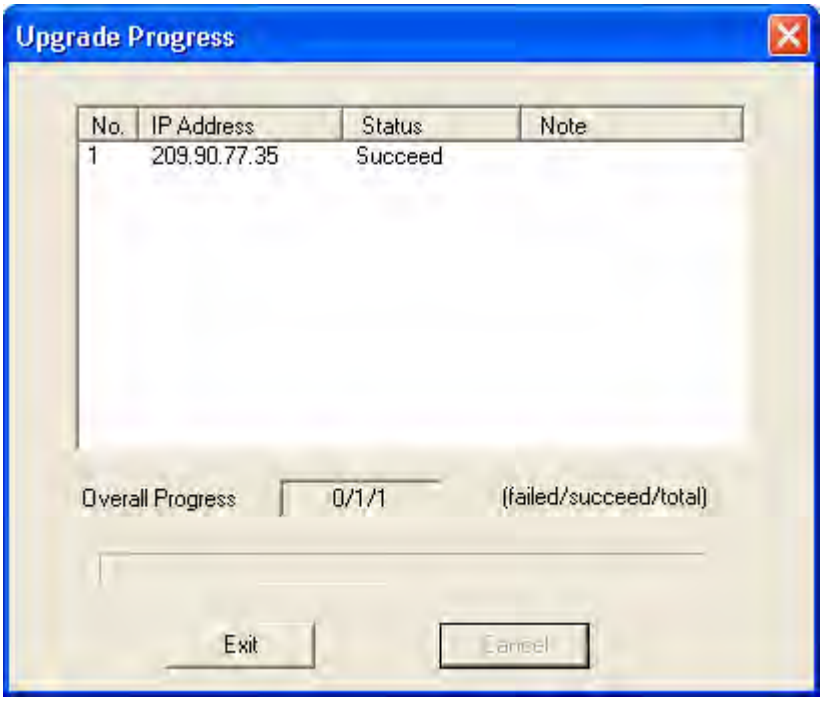
5 Select the time to perform the upgrade. You can either send the update file immediately or select a specific time and date to send the file. You may, for example, want to perform an upgrade during off hours such as a weekend.

6 Click Next and a window like this will appear:



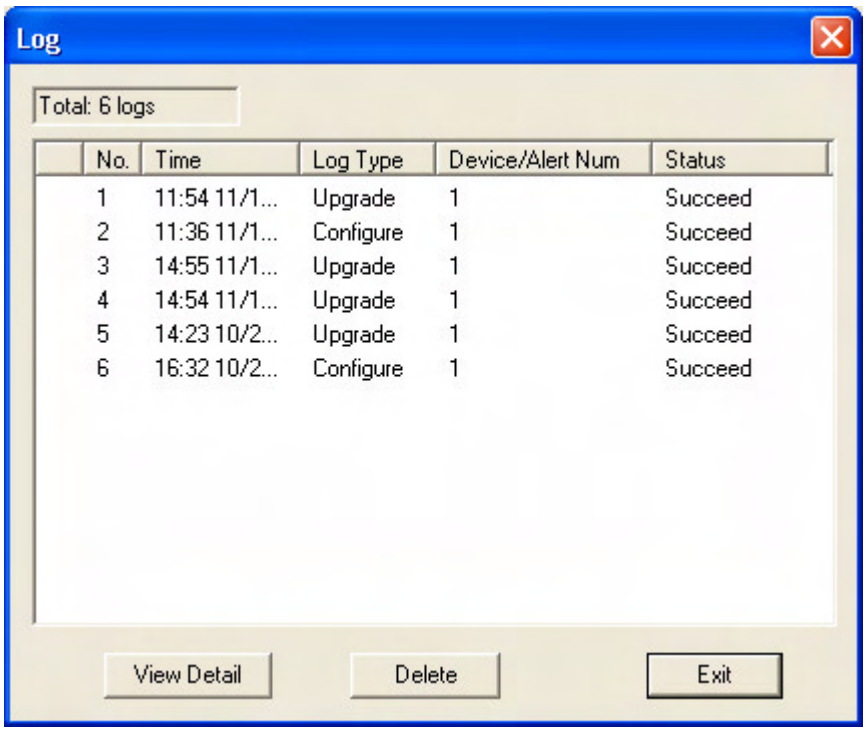
7 Review the list of IntelliJacks you want to upgrade. If you want to modify this list, click Cancel and restart the firmware upgrade procedure.

8 Type your password in the Password field, then click Finish. The Upgrade Progress dialog box will appear.



Viewing Log Files

The Central Configuration Manager creates a log file with details of the firmware upgrades, configuration operations, and alert messages from the IntelliJack. This file is in the Central Configurator\Log subdirectory under the directory where you installed the IntelliJack configuration software. You can the log by selecting Log History from the View menu. A window like this will appear:

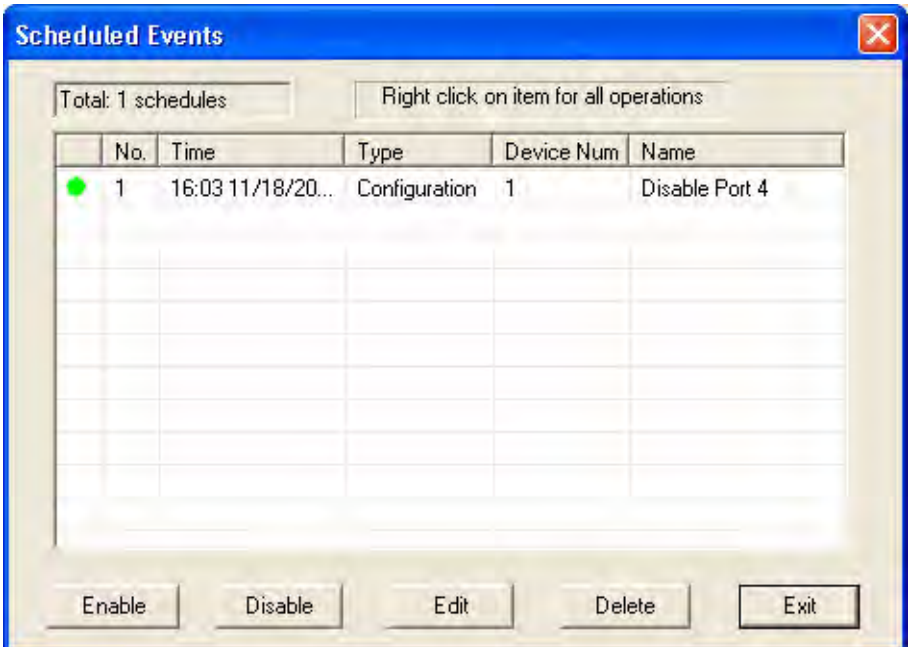


To view the details of a particular log, select it and click Detail. If an upgrade or configuration operation fails for some reason, a message will appear in the log file. Consult the troubleshooting guide on page 65 for more information.

Viewing and Canceling Scheduled Firmware Upgrades

You can select a time and date to send an upgraded firmware image to the IntelliJacks in your network. To view and make changes to the firmware upgrades you have scheduled, follow these steps:

1 Select Manage Schedule from the Tools menu. A window like this will appear:



2 To view the details of a scheduled upgrade, select it from the list and click Show Devices. To cancel a scheduled upgrade, select it from the list and click Delete.

A Troubleshooting the NJ220

If you encounter problems with the IntelliJack:

- Verify the IntelliJack is receiving power by viewing the Power LED (it should be on). If the Power LED is not on, make sure that:
  - If using power over Ethernet, the other end of the network cable is plugged into a switch on the network that has Power Over Ethernet integrated into it, or one that feeds into an external midspan power supply that supports Power Over Ethernet.
  - The local power supply is plugged into the IntelliJack and into a working electrical outlet, if your network does not support Power Over Ethernet.
- Verify the IntelliJack is connected to the network properly by viewing the Link LED (it should be on). If the Link LED is not on, make sure the network cable:
  - Is terminated properly. Refer to the connector manufacturer's instructions for terminating the cable. Be sure to test the connector and verify it is working.
  - Has a valid connection to the network.
  - Adheres to proper length and cabling specifications for your network.
- The IntelliJack is configured for manual MDI. Be sure to use a straight-through cable. If you want to use a cross-connect cable, you must change settings in the Configuration Manager software.

Troubleshooting Matrix

Event/Message	Description	Solution
Power LED is not on	IntelliJack is not receiving power	■ Ensure power supply is properly connected. ■ For power over Ethernet, make sure that the cable is connected to both the LAN port on the back of the IntelliJack and to the workgroup switch. ■ Make sure the upstream switch is configured and active
Link LED is not on	IntelliJack has no connection to the network	■ Make sure network cable is properly terminated. ■ Make sure the IntelliJack is connected to the network. ■ Make sure the cable is plugged into the workgroup switch. ■ Make sure the upstream switch is configured and active

Event/Message	Description	Solution
Green LEDs on Ports 1-4 are not on	Network device has no connection to IntelliJack	■ Make sure the cable is properly connected to the network device. ■ Make sure the cable is firmly connected to one of the four IntelliJack ports labeled 1-4. ■ Make sure the cable is a good straight-through cable.
Amber LED on Port 1 is not lit	Power is not being forwarded to network device	■ Make sure the cable is properly connected to Port 1 of the IntelliJack. ■ Make sure the cable is properly connected to the powered device. ■ Make sure the IntelliJack is configured to match the cable - either straight through or crossover. ■ Make sure the powered device is IEEE 802.3af compatible. ■ Make sure the power requirement for the powered device does not exceed 7 watts. The IntelliJack can only forward up to 7 watts.
Power LED is blinking continuously	Unit has detected a problem. Traffic can pass through, but management will not work.	■ Contact 3Com Technical Support.
Authentication Failure	Wrong password has been entered	■ Confirm correct password and re-type.
Timeout	Device did not respond within a specified period of time	■ Refresh the screen after a few seconds. If the problem persists, try to rediscover the device.
Attributes Error	Unexpected configuration parameters	■ Confirm that you have specified valid parameter values and retry the configuration operation. ■ NOTE: This error should not appear to the user under normal conditions.
General Error	Something other than authentication failure, timeout or attributes error has occurred	■ Retry the operation you were performing. ■ NOTE: This error should not appear to the user under normal conditions.

B Obtaining Support for Your 3Com Products

3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at:

http://eSupport.3com.com/

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

3Com offers the following support tool:

- **3Com Knowledgebase —** Helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

  http://knowledgebase.3com.com

  It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the

success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

http://www.3com.com/

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

You are entitled to *bug fix* / *maintenance releases* for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

http://eSupport.3com.com/

To obtain software releases that *follow* the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

Contact Us

3Com offers telephone, internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

http://eSupport.3com.com/

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at http://eSupport.3com.com/. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:
http://csoweb4.3com.com/contactus/

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim — Telephone Technical Support and Repair			
Australia	1800 075 316	Philippines	1800 144 10220 or 029003078
Hong Kong	2907 0456		
India	000 800 440 1193	PR of China	800 810 0504
Indonesia	001 803 852 9825	Singapore	800 616 1463
Japan	03 3507 5984	South. Korea	080 698 0880
Malaysia	1800 812 612	Taiwan	00801 444 318
New Zealand	0800 450 454	Thailand	001 800 441 2152
Pakistan Call the U.S. direct by dialing 00 800 01001, then dialing 800 763 6780 Sri Lanka Call the U.S. direct by dialing 02 430 430, then dialing 800 763 6780 Vietnam Call the U.S. direct by dialing 1 201 0288, then dialing 800 763 6780			
You can also obtain non-urgent support in this region at this email address apr_technical_support@3com.com Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048, or send an email at this email address: ap_rma_request@3com.com			
Europe, Middle East, and Africa — Telephone Technical Support and Repair			
From anywhere in these regions not listed below, call: +44 1442 435529			
From the following countries, call the appropriate number:			

Country	Telephone Number	Country	Telephone Number
Austria	0800 297 468	Luxembourg	800 23625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 4411 357
France	0800 917959	Portugal	800 831416
Germany	0800 182 1502	South Africa	0800 995 014
Hungary	06800 12813	Spain	900 938 919
Ireland	1 800 553 117	Sweden	020 795 482
Israel	180 945 3794	Switzerland	0800 553 072
Italy	800 879489	U.K.	0800 096 3266

You can also obtain support in this region using this URL: http://emea.3com.com/support/email.html

You can also obtain non-urgent support in this region at these email addresses:
Technical support and general requests: customer_support@3com.com
Return material authorization: warranty_repair@3com.com
Contract requests: emea_contract@3com.com

Latin America — Telephone Technical Support and Repair

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

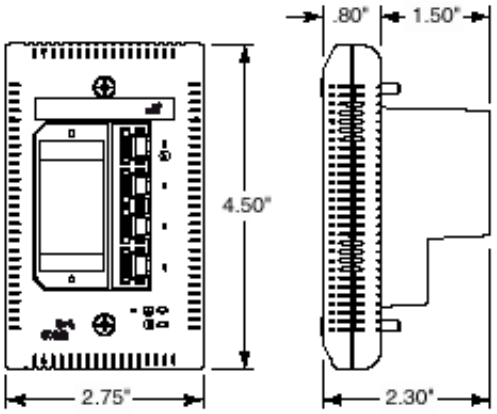
You can also obtain support in this region in the following ways:

- Spanish speakers, enter the URL: http://lat.3com.com/lat/support/form.html
- Portuguese speakers, enter the URL: http://lat.3com.com/br/support/form.html
- English speakers in Latin America, send e-mail to: lat_support_anc@3com.com

US and Canada — Telephone Technical Support and Repair

All locations:	All 3Com products:	1 800 876 3266

C Product Specifications



Hardware	
Power consumption	<5 watts without power forwarding Maximum 13 watts with power forwarding (depending on the device drawing power)
Network Interface	
10 Mbps Ethernet 10BASE-T	Ethernet IEEE 802.3 industry standard for a 10 Mbps baseband CSMA/CD local area network
100 Mbps Ethernet 100BASE-TX	Ethernet IEEE 802.3u industry standard for a 100 Mbps baseband CSMA/CD local area network
Performance	
Auto-negotiation	Communication speed (10 Mbps or 100 Mbps) and duplex mode (full or half) can be determined through auto-negotiation with the attached devices. The IntelliJack attempts to negotiate the fastest connection possible (100 Mbps full-duplex). The communication speed and duplex mode can also be controlled using the configuration management software.

MIB Support	MIB II (RFC 1213)
	Bridge MIB (RFC 1493)
	Ether-like MIB (RFC 1643)
	MIB for MAUs (RFC 2668)
	MIB for bridge with extensions (RFC 2674)
	802.1x MIBs
	RADIUS Authentication Client MIB (RFC 2618)
	RADIUS Accounting Client MIB (RFC 2620)
3Com Proprietary MIBs	Backup & Restore MIB
	RADIUS Client MIB
Standard Traps	Link Up
	Link Down
	Cold Start
	Authentication Failure
Proprietary Traps	SecureLogon
	SecureLogoff
	SecureLoginFailure
Environment	
Operating temperature	32° to 104° F (0° to 40° C)
Storage temperature	-22° to 194° F (-30°- to 90° C)
Operating humidity	10-90% noncondensing
Storage humidity	10-90% noncondensing
Operating Altitude	8,000 ft. max
Storage Altitude	20,000 ft. max
Standards Conformance	
IEEE802.3 10BASE-T, 100BASE-TX and auto-negotiation	
Power Over Ethernet (Capacitive Power Discovery Process and IEEE 802.3af)	
Power forwarding (IEEE802.3af; 7 watts, 48 volts)	
Features	
Power Over Ethernet	Compatible with IEEE 802.3af and Capacitive Power Discovery Process
Local power supply	Required for networks that do not support Power Over Ethernet
Voice Over IP (VoIP)	Compatible with VoIP standard.

Power forwarding	Power forwarding Port number 1 can be used with any standard networking device as well as to power a device such as a VoIP telephone on a network that uses IEEE 802.3af-compatible Power Over Ethernet.

RMON Counters

InUnicasts	Total valid frames received with a unicast Destination Address. A valid frame has a good FCS and its size is greater than 64 bytes and less than 1518 for non tagged frames, 1522 for tagged frames, or 1535 if MaxFrameSize =1 (set in global control register).
InBroadcasts	Total valid frames received with destination address equal to FF:FF:FF:FF:FF:FF.
InPause	Total pause frames received.
InMulticasts	Total valid frames received with multicast destination address that are not counted in InBroadcasts or InPause.
InFCSErr	Total frames received with a valid length and an invalid FCS.
AlignErr	Total frames received with valid length that have an invalid FCS and a non-integral number of octets.
InGoodOctets	Total data octets received in frames with a valid FCS. Undersize and oversize frames are included. The count includes the FCS but not the preamble.
InBadOctets	Total data octets received in frames with an invalid FCS; fragments and jabbers are included, The count includes the FCS but not the preamble.
Undersize	Total frames received with a length of less than 64 octets but a valid FCS.
Fragments	Total frames received with a length of less than 64 octets and an invalid FCS
In64Octets	Total frames received with a length of exactly 64 octets, including those with errors.
In127Octets	Total frames received with a length of between 65 and 127 octets inclusive, including those with errors.
In255Octets	Total frames received with a length of between 128 and 255 octets inclusive, including those with errors.
In511Octets	Total frames received with a length of between 256 and 511 octets inclusive, including those with errors.
In1023Octets	Total frames received with a length of between 512 and 1023 octets inclusive, including those with errors.
InMaxOctets	Total frames received with a length of between 1024 and MaxSize octets inclusive, including those with errors.
Jabber	Total frames received with a length of more than MaxSize octets but with an invalid FCS.
Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS.

InDiscards	Total valid frames received that are discarded due to lack of buffer space. This includes frames discarded at ingress as well as those dropped due to priority and congestion considerations at the output queues. Frames dropped at egress due to excessive collisions are not included but are counted in the Excessive counter.
InFiltered	If 802.1Q is disabled on the port, these are the total valid frames received that are not forwarded to a destination port. These are frames for which the destination port vector is 0 or are not forwarded due to the state of the portState bits. valid frames discarded due to a lack of buffer space are not included. If 802.1Q is enabled on the port, then these are the total valid frames received (tagged or untagged) that were discarded due to an unknown VID (i.e., the frame's VID was not in the VTU)
OutUnicasts	Total valid frames transmitted with a unicast destination address
OutBroadcasts	Total valid frames transmitted with destination address equal to FF:FF:FF:FF:FF:FF.
OutPause	Total pause frames transmitted.
OutMulticasts	Total valid frames transmitted with multicast destination address that are not counted in OutBroadcasts or OutPause.
OutFCSErr	Total frames transmitted with a valid length and an invalid FCS.
OutGoodOctets	Total data octets transmitted. The count includes the FCS but not the preamble.
Out64Octets	Total frames transmitted with a length of exactly 64 octets, including those with errors.
Out127Octets	Total frames transmitted with a length of between 65 and 127 octets inclusive, including those with errors.
Out255Octets	Total frames transmitted with a length of between 128 and 255 octets inclusive, including those with errors.
Out511Octets	Total frames transmitted with a length of between 256 and 511 octets inclusive, including those with errors.
Out1023Octets	Total frames transmitted with a length of between 512 and 1023 octets inclusive, including those with errors.
OutMaxOctets	Total frames transmitted with a length of between 1024 and 1522 octets inclusive, including those with errors.
Collisions	Total number of collisions during frame transmission.
Late	Total number of times collision is detected later than 512 bit-times into the transmission of a frame.
Excessive	Total number of frames not transmitted because the frame experienced 16 transmission attempts and was discarded. The discard will only occur if DiscardExcessive is set to a 1 (in global control register).
Multiple	Total number of successfully transmitted frames that experienced more than on collision.

Single	Total number of successfully transmitted frames that experienced exactly one collision.
Deferred	Total number of successfully transmitted frames that are delayed because the medium is busy during the first attempt.

REGULATORY INFORMATION

FCC COMPLIANCE

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC CLASS A VERIFICATION STATEMENT

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

INDUSTRY CANADA (IC) COMPLIANCE STATEMENT

This Class A digital apparatus complies with Canadian ICES-003.

AVIS DE CONFORMITÉ À LA RÉGLEMENTATION D'INDUSTRIE CANADA

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

EUROPEAN UNION DECLARATION OF CONFORMITY

This product is in compliance with the essential requirements and other relevant provisions of Directives 73/23/EEC and 89/336/EEC.

CE

JAPAN VCCI COMPLIANCE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Translation:

This is a Class A product based upon the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.