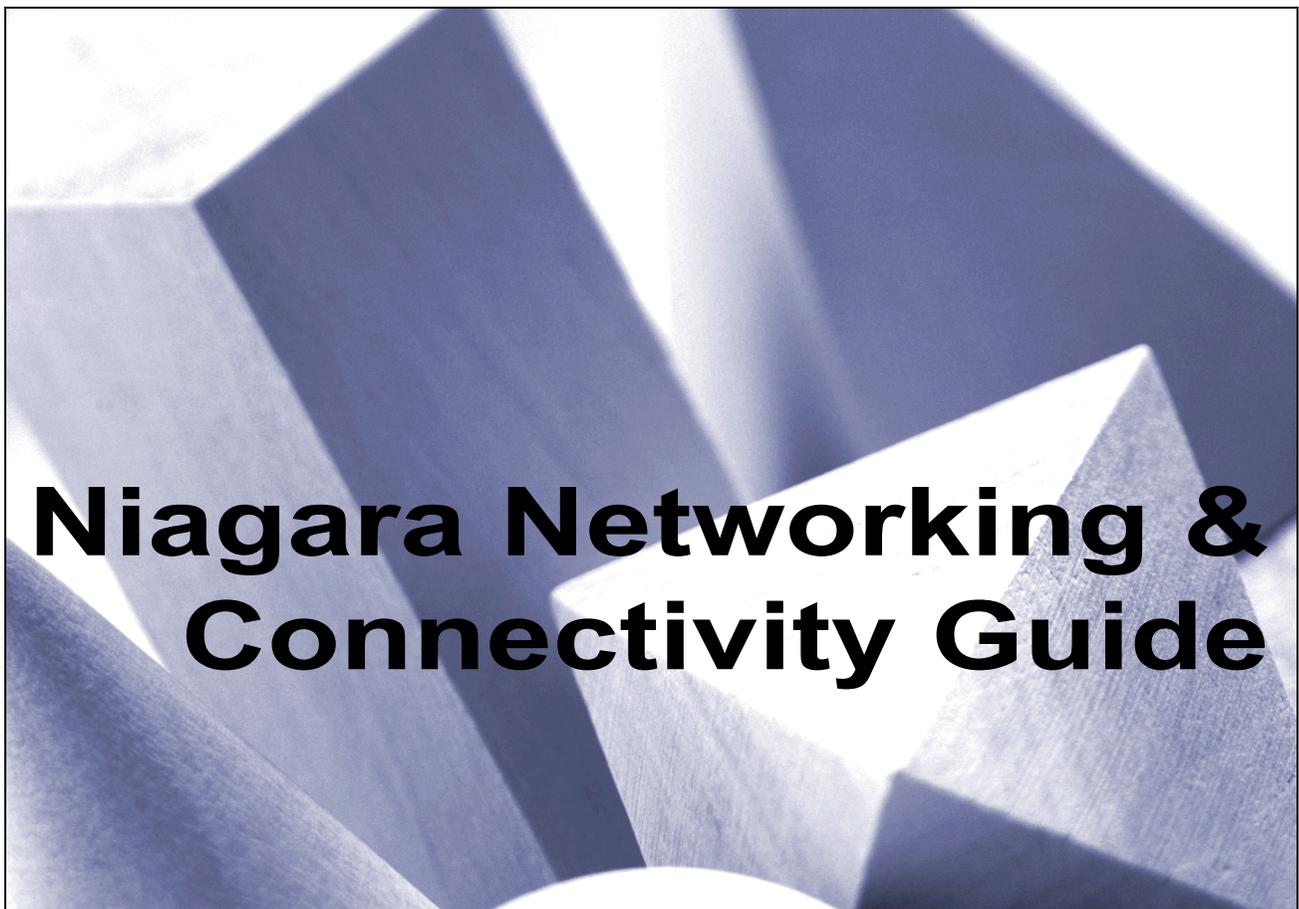




Technical Publications



Niagara Networking & Connectivity Guide

Tridium, Inc.
3951 Westerre Parkway • Suite 350
Richmond, Virginia 23233
USA

<http://www.tridium.com>
Phone 804.747.4771 • Fax 804.747.5204



Copyright Notice: The software described herein is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

© 2002 Tridium, Inc.
All rights reserved.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc., 3951 Westerre Parkway, Suite 350, Richmond, Virginia 23233.

The confidential information contained in this document is provided solely for use by Tridium employees, licensees, and system owners. It is not to be released to, or reproduced for, anyone else; neither is it to be used for reproduction of this control system or any of its components.

All rights to revise designs described herein are reserved. While every effort has been made to assure the accuracy of this document, Tridium shall not be held responsible for damages, including consequential damages, arising from the application of the information given herein. The information in this document is subject to change without notice.

The release described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademark Notices: Metasys is a registered trademark, and Companion, Facilitator, and HVAC PRO are trademarks of Johnson Controls Inc. Black Box is a registered trademark of the Black Box Corporation. Microsoft and Windows are registered trademarks, and Windows 95, Windows NT, Windows 2000, and Internet Explorer are trademarks of Microsoft Corporation. Java and other Java-based names are trademarks of Sun Microsystems Inc. and refer to Sun's family of Java-branded technologies. Communicator and Navigator are registered trademarks of Netscape Communications Corporation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium Niagara, the Niagara Framework, Vykron, WorkPlace Pro, Java Desktop Environment, Web Supervisor, JACE-4, JACE-5, and JACE-NP are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks have been appropriately capitalized and are the properties of their respective owners.

Niagara Networking & Connectivity Guide

© 2002, Tridium, Inc.
All rights reserved.



CONTENTS

PREFACE

About This Document	xii
Intended Audience	xii
Prerequisite Knowledge	xiii
Document Summary	xiii
Formatting Conventions	xiii
Special Notations	xiv
Related Documentation	xiv
Sources	xiv

CHAPTER 1

Understanding Networking and IP Addressing	1-1
Introduction to Networking	1-1
What is Networking?	1-2
The Concept of Networking	1-2
Types of Networks	1-3
Server-based Networks	1-3
Peer-to-peer Networks	1-3
Specialized Servers	1-3
Network Design	1-3
Standard Topologies	1-3
Hubs	1-6
Network Cabling	1-7
Wireless Network Communications	1-8
Network Interface Card	1-8
Connectors	1-9
The OSI Model and the IEEE 802 Standards	1-9
The OSI Model	1-9
Layered Architecture	1-9
The IEEE 802 Standards	1-10
Drivers	1-11
Protocols	1-11
How Protocols Work	1-12

Protocols and the OSI Model	1-12
Access Methods	1-13
Contention Methods	1-13
Token Passing	1-13
Polling	1-14
Expanding Networks	1-14
Repeaters	1-14
Bridges	1-15
Routers	1-15
Brouters	1-16
Gateways	1-16
Networking using IP	1-16
What is IP?	1-17
The OSI Model and TCP/IP	1-17
IP Addressing	1-19
What is an IP Address?	1-19
IP Classes	1-19
Network (Subnet) Masks	1-20
Special IP Addresses	1-22
IP Address Allocation	1-23
Private IP Addresses	1-23
Network Address Translation (NAT)	1-23
IP Routing and Default Gateway	1-24
Static and Dynamic IP Addressing	1-25
Associating IP Addresses with Host Names	1-26
The HOSTS File	1-26
DNS	1-27
WINS	1-28
DDNS	1-28
Proxy Servers and Firewalls	1-28
Proxy Server	1-28
Firewall	1-29
About Ports	1-31
Niagara Considerations	1-32
Niagara Hosts	1-32
Available Networking Technologies	1-33
Communication between Niagara Hosts	1-35

	Additional Information	1-36
CHAPTER 2	Configuration and Troubleshooting Tools	2-1
	Niagara Configuration Tools	2-1
	Admin Tool	2-1
	JACE-NP Remote Control Utilities	2-2
	NetMeeting	2-2
	Remote Command Utility	2-5
	Hyperterminal	2-7
	About the VxWorks Target Shell	2-8
	About Serial and Null Modem Cables and Adapters	2-12
	Telnet	2-14
	Enabling Telnet on a JACE-4/5	2-14
	Connecting with Windows Telnet	2-15
	Using Hyperterminal to Telnet	2-16
	FTP	2-17
	Connectivity Troubleshooting Utilities	2-19
	Using Windows Command-line Utilities	2-20
	Opening a Command Prompt	2-20
	TCP/IP Utilities	2-20
	ping	2-20
	tracert	2-22
	nslookup	2-23
	netstat	2-25
	Windows-specific	2-27
	ipconfig	2-27
	Additional Information	2-29
CHAPTER 3	Connecting on a LAN	3-1
	Niagara Considerations	3-1
	System Architectures	3-1
	Single site	3-1
	Multiple sites	3-3
	Things to Note	3-4
	Using Niagara in a Microsoft Windows Server Environment	3-4
	Windows NT and Windows 2000 Security	3-5
	Connecting an Engineering PC	3-6

Windows NT 4.0	3-6
Windows 2000	3-8
Connecting a New JACE Controller	3-9
Determining the Default Network Information	3-10
About Ethernet Straight Through and Crossover Cables	3-10
Connecting to the LAN and Assigning the IP Address	3-12
Crossover Cable Connection	3-14
Troubleshooting Connectivity to an Existing JACE Controller	3-14
Determining Network Settings	3-16
About the ipchanges.txt file	3-16
JACE-NP	3-17
JACE-4/5	3-19
Other Access Methods	3-21
JACE-NP	3-21
JACE-4/5	3-21
Using DHCP	3-23
Niagara Considerations	3-23
Determining the MAC Address	3-23
Using DHCP on a JACE-4/5	3-24
Configuring the JACE-4/5	3-25
Troubleshooting DHCP Problems on the JACE-4/5	3-26
Using DHCP on a Windows-based Niagara Host	3-29
Configuring an Engineering PC	3-30
Configuring a JACE-NP	3-30
Troubleshooting DHCP Problems on the JACE-NP	3-30
CHAPTER 4	
Connecting with Direct Dial	4-1
Niagara Considerations	4-1
System Architectures	4-2
About Dialing between Niagara Hosts	4-3
User- versus Application-initiated Connections	4-4
Design Considerations	4-5
Configuring Direct Dial on the JACE-4/5	4-7
Installing and Configuring Modems	4-7
About Pre-configured Modems	4-7
Enabling the JACE-4 Modem (Internal or External)	4-10
Attaching an External Modem	4-11

Configuring the Software	4-12
About the ras.properties File	4-12
Configuring ras.properties for Direct Dial	4-14
Enabling Dial-in	4-16
Configuring Direct Dial on the JACE-NP	4-17
Installing and Configuring Modems	4-17
Supported Modems.	4-17
Installing an External Modem	4-17
Installing the Modem Driver	4-17
Configuring the RAS Software	4-20
Configuring RAS	4-20
Starting RAS.	4-24
Granting Dial-in Permissions	4-25
Configuring Direct Dial on an Engineering PC	4-25
Installing and Configuring Modems	4-26
Supported Modems.	4-26
Installing an External Modem	4-26
Installing the Modem Driver	4-26
Installing and Configuring the RAS Software	4-27
Installing the RAS Software (Windows NT 4.0 only)	4-27
Configuring RAS	4-28
Starting RAS (Windows NT 4.0 only)	4-31
Granting Dial-in Permissions	4-31
Using Direct Dial.	4-32
Configuring the Station for Dial-out.	4-32
Making a User-initiated Connection from an Engineering PC.	4-34
Creating the DUN Connection	4-35
Establishing the Connection.	4-39
Accessing the Host or Station	4-43

CHAPTER 5	Connecting to an ISP	5-1
	Niagara Considerations	5-1
	System Architectures	5-2
	Additional Scenarios	5-3
	About Connecting to an ISP	5-5
	Design Considerations	5-6
	Selecting an ISP	5-7

Configuring Captive ISP on the JACE-4/5	5-8
About Captive ISP	5-8
About Disconnects	5-8
Installing and Configuring Modems	5-9
Configuring the Software	5-9
Information Required from the ISP	5-9
Configuring Network Settings for Captive ISP	5-9
Configuring ras.properties for Captive ISP	5-10
Granting Dial-in Permissions	5-15
Using the IspConnection Object to Control Disconnects	5-15
E-mail Configuration	5-19
Troubleshooting Connection Problems	5-19
Avoiding Automatic Disconnects	5-21
Configuring DDNS on the JACE-4/5	5-22
About TZO	5-22
Registering with TZO	5-22
Configuring the JACE-4/5 for DDNS	5-23
About the ddns.properties file	5-23
Configuring the ddns.properties file	5-23
Troubleshooting DDNS Connections	5-24
Troubleshooting Update Failures	5-25
Connecting Windows-based Hosts via Telephone Modem	5-26
Configuring the JACE-NP	5-26
Configuring a Web Supervisor	5-26
Connecting via Cable or DSL Modem	5-27

CHAPTER 6	Using Security Technologies	6-1
	Security Considerations	6-1
	Creating a Strong Password	6-3
	Using a Firewall or Proxy Device	6-4
	Default Niagara Port Numbers	6-7
	Changing Niagara Default Ports	6-9
	Changing the Station HTTP Port (80)	6-9
	Changing the Administration Port (3011)	6-12
	Changing the Time Synchronization Port	6-17
	Impact of Changing Default Niagara Ports	6-18
	Additional Open Ports on the JACE-NP	6-20

Disabling Open Ports on Microsoft Windows NT 4.0	6-22
Using a Virtual Private Network	6-23
Niagara System Architectures	6-24
Things to Note.	6-24

APPENDIX A	Configuration Files Used for Communication	A-1
	Windows-based Niagara Hosts	A-1
	JACE-4/5	A-2



About This Document

This document is intended to help you connect Niagara hosts to:

- Ethernet networks using IP
- each other, directly through modems
- an ISP for connectivity to other hosts

Included are procedures for getting started, station engineering considerations, reference information on networking and IP addressing, troubleshooting tips, and information on network security with Niagara hosts.

This preface includes the following sections:

- [Intended Audience](#)
- [Prerequisite Knowledge](#)
- [Document Summary](#)
- [Formatting Conventions](#)
- [Special Notations](#)
- [Related Documentation](#)

Intended Audience

The following people should use this document:

- Vykon systems integrators responsible for selling jobs into diverse customer environments.
- Vykon systems integrators and installers responsible for initial setup and ongoing configuration of JACE controllers and Web Supervisors.
- IT managers who want to understand how Niagara hosts interoperate in their environment.

Prerequisite Knowledge

To get the most from this guide, you should know or have experience with the following:

- Basic Niagara concepts, such as stations, nodes, objects, properties and links.
- The JDE (Java Desktop Environment), including necessary tasks to provide system control. Ideally, you should be Niagara-certified, that is, have successfully passed Tridium's Niagara TCP (Technical Certification Program).
- Niagara controllers and Web Supervisors.

Document Summary

This document contains a six chapters, one appendix, a glossary, and an index. The main chapters and appendixes contain the following information:

- [Chapter 1, “Understanding Networking and IP Addressing”](#)—Provides an overview of networking and IP addressing, including an overview of networking and Niagara hosts.
- [Chapter 2, “Configuration and Troubleshooting Tools”](#)—Discusses the tools used to set up networking on Niagara hosts and to troubleshoot connectivity issues.
- [Chapter 3, “Connecting on a LAN”](#)—Discusses how to connect Niagara hosts to a Local Area Network (LAN).
- [Chapter 4, “Connecting with Direct Dial”](#)—Talks about how to connect Niagara devices directly to each other using modems.
- [Chapter 5, “Connecting to an ISP”](#)—Discusses how to connect Niagara hosts through an ISP to other hosts.
- [Chapter 6, “Using Security Technologies”](#)—Gives information on using security with Niagara hosts.
- [Appendix A, “Configuration Files Used for Communication”](#)—Provides a list and purpose for configuration files used on Niagara hosts.

Formatting Conventions

This document uses text formatting conventions to convey the following specific meanings.

- **Bold text** indicates an important keyword, a keyboard key name, or an interface object name. Examples:
 - the **ENTER** key
 - the **File** menu
 - Type `nre tridiumx.eas.demo.EasDemoGen station` where **station** is the name of the station you created.

- *Italic text* is used to refer to the titles of other publications. Examples:
 - *The Microsoft Manual of Style*
 - *Niagara Web Solutions Guide*
- *Italic text* is also used for non-literal text that represents a variable. Examples:
 - *station_name*
 - *DONOFF_n*
- *Italic text* is sometimes used to call attention to a specific word or concept. Example:
 - the *backed-up* station database
- Bold text in a different font is used for **extreme emphasis** of a specific word or concept.
- CAPITAL letters are used for acronyms, such as JDE (Java Desktop Environment). They are also used to identify keyboard keys in instructions. Examples:
 - Press **ENTER**.
 - Press **CTRL+C**.
 - Open the JDE.
- “Quotation marks” are used to refer to the names of sections within the current document. Examples:
 - “[Formatting Conventions](#)” contains style and usage meanings.
 - For additional information, see the “[Sources](#)” section on page xiv.
- <Text between brackets> is used as a placeholder for user-supplied values. Examples:
 - <password>
 - <userid>
- <**Bold text between brackets**> is used to indicate a variable in contexts where italic text is not appropriate or is not easily discernible from other text. Example:
 - D:\niagara**<Niagara release number>**\stations

Special Notations

The following special notations alert readers to additional information related to the main text.



Note

Notes typically contain additional details that are not mentioned within the body of the text. They alert readers to important information that might otherwise be overlooked.

**Tip**

Tips typically contain best practices, recommendations, or other helpful instructions that help the reader use the product more effectively.

**Timesaver**

Timesavers typically tell readers about a quicker or shorter way to perform a task. They point out keyboard combinations, buttons, or shortcuts that readers can use instead of menu selections or keystrokes to perform the same action.

**Caution**

Cautions remind the reader to be very careful. They alert readers to situations where there is a chance of performing an action that cannot be undone, might cause unexpected results, or might cause data loss. Cautions contain an explanation of why the action is potentially problematic.

**Warning**

Warnings alert the reader to proceed with extreme care. They alert readers to situations where there is a risk of personal injury or equipment damage. Warnings contain an explanation of why the action or situation is potentially dangerous.

Related Documentation

For additional information, refer to the following other Niagara Technical Publications:

- *Niagara Standard Programming Guide*, revised December 18, 2001, Tridium, Inc.
Provides property-level reference information on all standard Niagara objects, including Gx and GxPage types.
- *Niagara Quick Start Guide*, revised November 15, 2001, Tridium, Inc.
Provides an introduction to using the Niagara Framework applications installed on a Web Supervisor.

Sources

The following source was used in the preparation of this document, and is gratefully acknowledged:

- *Niagara Web Solutions Guide*, revised December 18, 2001, Tridium, Inc., www.tridium.com.
- *Niagara Standard Programming Reference*, revised April 18, 2002, Tridium, Inc., www.tridium.com.



Understanding Networking and IP Addressing

This chapter gives a concise overview of networks and IP addressing, as a guide to the terms and concepts used in later chapters. It does this with these main topics:

- [Introduction to Networking](#)
- [Networking using IP](#)
- [Niagara Considerations](#)
- [Additional Information](#)

Introduction to Networking

To understand connecting Niagara devices, one must first understand the basics of network communications. Therefore, this topic serves as an introduction to networking and it includes the following discussions:

- [What is Networking?](#)—what networks are and how they are used.
- [Types of Networks](#)—includes peer-to-peer networks, server-based networks, and various other server-based networks.
- [Network Design](#)—describes various network topologies and the equipment used to build a network.
- [The OSI Model and the IEEE 802 Standards](#)—discusses the concept of dividing network communications into separate layers.
- [Drivers and Protocols](#)—describes network interface drivers and how protocols work.
- [Access Methods](#)—describes how computers handle instances where multiple transmitters attempt to send messages at the same time.
- [Expanding Networks](#)—discusses devices used to expand networks, including repeaters, bridges, routers, brouters, and gateways.

What is Networking?

This section introduces LANs and WANs and how networks are used to improve computing productivity.

The Concept of Networking

A network is simply a method by which computers and/or devices can communicate over a common connection. This means that whether you have 2 PCs, 20 PCs, or 200 PCs, they can all communicate with each other via the network.

Local Area Network (LAN)

A LAN usually refers to computers connected so they can share resources and interoperate within a small area such as an office or a single building.

Wide Area Networks (WAN)

The need to communicate with PCs and other devices outside of the office or local network has led to the expansion of networks into wider circles of connectivity. Devices are added to LANs that enable them to communicate with remote devices. This is accomplished by the use of modems, routers, public switched telephone networks (PSTN), bridges, and so on. These devices extend the communication capabilities of the LAN into a wide area network.

Why Use a Network?

When there is a need to share data and resources between multiple users or PCs, connecting all these PCs using some type of network is a common sense choice for effective utilization of the available assets.

Printers and other peripherals—When there is a network, one printer can support an entire team with printing services from a common location. Each PC is configured to use the printer as if it belonged to that PC alone. This allows an organization to buy a small number of high-speed, high-quality printers that are used to support everyone. The savings realized by buying fewer printers can then be used to substantially increase the quality of the equipment purchased for use by the group.

Data—The sharing of data between multiple users is also a highly valuable commodity: One common database can be accessed from anywhere in the organization and all users can view and make changes to the same data. Using a server PC to store documents, templates, and clipart that multiple persons may need access to is a very important benefit of using a network.

Applications—Another good reason for a network is to run applications software across the network from a single installation. Most enterprise-level software applications can be purchased specifically for network operation. Multi-user licensed software is usually much less expensive than purchasing individual copies of software. In addition, running applications across the network ensures that everyone is using the same version of the software, so there is never a document compatibility problem.

Types of Networks

The evolution of PC networking technology started with specialized disk servers that ran special operating systems (OSs) supporting simultaneous file access from a group of clients. The biggest drawback to this design is that it requires a powerful computer dedicated to running the network operating system. Over time, this approach has evolved into one where each PC on the network can be both client and server: Today, individual PCs can be configured so users on other PCs can access specific areas on their disk and use devices to which they are connected. Because any client can be a file server and any server can be a client, the systems are considered to have peer status.

Server-based Networks

In a server-based network, the PCs that attempt to access the network are monitored by a central access control manager. Typically, a PC is given all information about the network users, which are each assigned user permissions, passwords, and access rights to the various resources on the network according to their needs. Users can be grouped (in user groups) to more easily manage their access privileges. The PC that has this management function is referred to as the logon server or domain controller, and it is possible for multiple PCs to share these server responsibilities.

Peer-to-peer Networks

Peer-to-peer networks involve PCs that manage their own network connection on the common media. In other words, logging onto the network and the resources that can be accessed on the network is a function that is managed by the PC that is connecting. All PCs are equal in priority—no one PC can prevent another PC from connecting to the network. In a peer-to-peer network, there is little or no network security offered—when a user logs onto the PC, they are automatically logged onto the network.

Specialized Servers

Often, specialized servers are used to perform server level functions on a network other than access control. These might include print servers, database servers, and application servers. In the Microsoft world, these are referred to as member servers. Normally, these PCs are not used as individual workstations that double as an application server—they typically sit off on the sidelines managing their resources, providing group connectivity.

Network Design

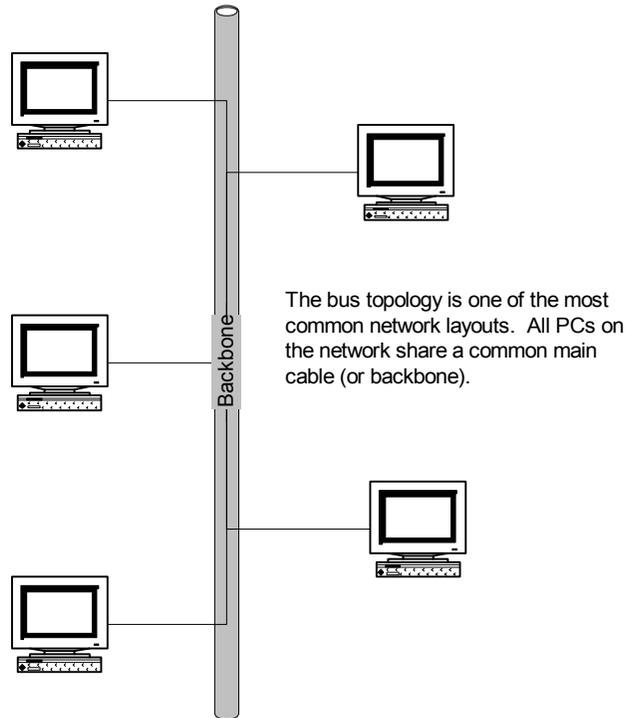
Networked PCs need some form of communications system that provides a fast and reliable transport system for messaging. This section discusses the hardware, cabling, and architecture used to support network communications.

Standard Topologies

The physical layout or description of a network is called topology. The three most common topologies are: bus, star, and ring. Combinations of these can also be used to create hybrid topologies.

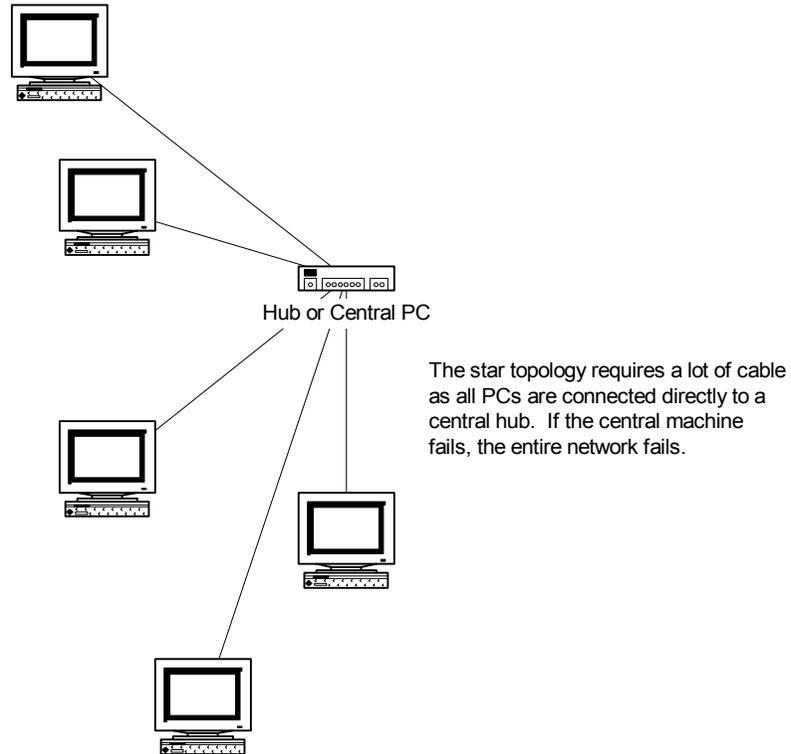
The bus topology uses a single **backbone** cable to which network devices connect. Devices are connected either directly to it or by way of a short drop cable. As message traffic passes along the network, each PC checks the message to see if it is directed to itself. Each end of the bus segment requires an end-of-line terminator.

Figure 1-1 Bus topology.



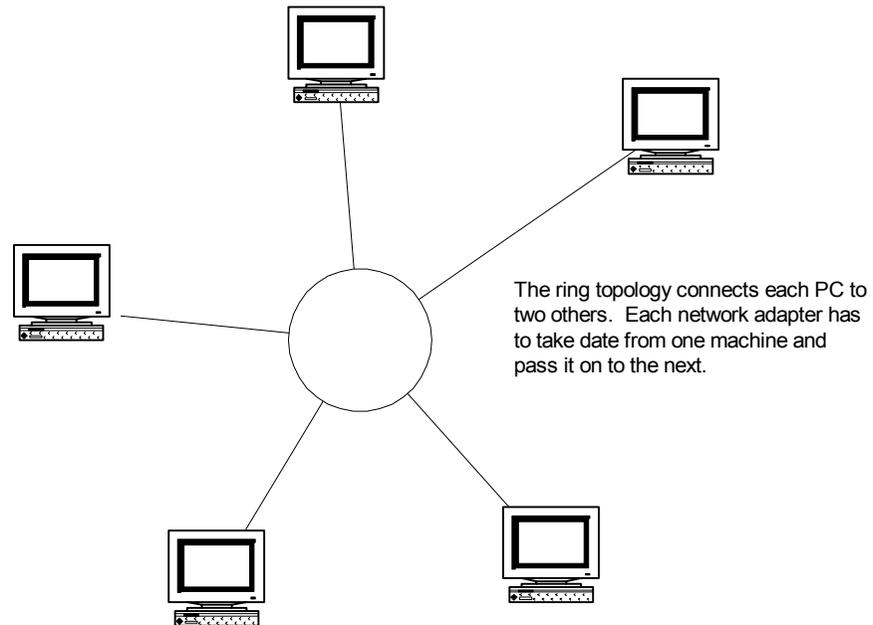
The star topology uses a central device called a hub to which each network device is connected. Network devices are connected point-to-point to the hub with a patch cable. All messages in a star topology are routed through the hub before reaching their final destination.

Figure 1-2 Star topology.



Ring topologies consist of several nodes joined together to form a circle. Messages move from one node to the next in one direction only: When a node receives a message that is addressed to itself, the message is copied and placed back on the network with a modification indicating that it was received.

Figure 1-3 Ring topology.



Hubs

When LANs were first developed, all computers were connected to a single cable that was strung from location to location. Not only was it difficult to add new computers to the LAN, but if there was a break in the cable, the whole LAN was disrupted. A hub is a hardware component that connects many cables in one device. They are used to break up the LAN into smaller point-to-point segments that support multiple networked resources. When using hubs, if any one segment has trouble, only computers on that segment are affected. Hubs also allow the network structure to change without restringing cable—simply add, move, or delete devices at the hub.

Hubs are mandatory in 10BASE-T twisted pair Ethernet as well as Token Ring networks.

- Active hubs have the ability to amplify a signal and retransmit it.
- Passive hubs simply pass a signal through without conditioning it.
- Intelligent hubs have switching and management capabilities that allow them to make choices as to which network path is used to transmit signals.
- Switching hubs (switches) can increase the number of PCs connected to a LAN by breaking it down into more manageable virtual segments. Whereas a hub requires all resources to share the bandwidth of the network, switching hubs give any two nodes on the network the full bandwidth of the line.

Network Cabling The transmission medium used to support network communications is an extensive subject. There are issues that define the best type of cable suited for different signaling rates, different physical and electrical environments, and various architectural requirements and limitations. The key is to strike an acceptable balance between performance, cost, and capacity.

Coaxial Cable

Coaxial cable contains a single, solid or stranded wire, inner conductor surrounded by an outer conductor surrounded by an outer conductor and shield of braided wire mesh or foil. The conductor and the shield are separated from each other by a layer of insulation, and the entire cable is wrapped in another layer of insulating material. Because the conductor and the shield share the same axis, the medium is called coaxial, or coax for short. Coaxial cable generally provides better protection from electromagnetic interference (EMI) than twisted pair cabling, but it is more expensive and tougher to work with.

Some network standards are compatible with more than one type of cable. Ethernet, for instance, can use either thick or thin coaxial cable. The thicker cable, called thick Ethernet or 10Base5—the 5 refers to a maximum segment distance of 500 meters—can reliably carry signals over greater distances than thin Ethernet, also called 10Base2, which can only stretch up to 185 meters. With 10Base2, a 50-ohm terminator is mounted at the host, whereas with 10Base5 the terminator is mounted on the cable. ThickNet cable tends to be more expensive than ThinNet cable and it uses RG-11 connectors, whereas ThinNet cable uses BNC connectors.

Twisted Pair Cable

Twisted pair cable has two insulated copper wires that are twisted around each other to reduce EMI (referred to as crosstalk). Twisted pair cable has been used for years in the telephone industry, so the technology and standards for this type of cable are well established. However, many standard telephone cables are not twisted pair and are inadequate for most network applications.

Although twisted pair cable is often unshielded, some products use shields to reduce the cable's susceptibility to EMI. When a distinction must be made, twisted pair cable may be referred to as either UTP (unshielded twisted pair) or STP (shielded twisted pair). STP is capable of handling more data at greater speed and is more resistant to outside interference.

The majority of new wiring installations use Category 5 UTP wire in order to be able to run faster network technologies. Categories 1 through 5 are based on the EAI/TIA-568 standard.

Table 1-1 Cable categories.

Category	Cable Type	Application
1	UTP	Analog voice
2	UTP	Digital voice (1 Mbps data)
3	UTP, STP	16 Mbps data
4	UTP, STP	20 Mbps data
5	UTP, STP	100 Mbps data

Table 1-1 Cable categories.

Category	Cable Type	Application
6	Coaxial	100 Mbps+ data
7	Fiber Optic	100 Mbps+ data

Fiber Optic Cable

Optical fiber transmits signals of light through a very fine strand of plastic or glass fiber, which is encased in a tube made of glass called cladding, surrounded by a tough outer sheath. The cladding is designed to reflect light back into the optical fiber, which causes the light to bounce from side to side as it moves through the optical fiber. There are single-mode cables (one optical fiber) and there are multi-mode cables. Multi-mode cables have several optical fibers grouped at the center, each providing a separate communications channel.

Wireless Network Communications

Wireless communications transmit data without the use of physical media (i.e., wire) and conduit. Wireless communications include radio transmissions, laser, infrared, and others. The greatest benefit of wireless communications is that the technology supports non-traditional network configurations.

Radio waves can be used to transmit to a number of devices throughout a building without concern for existing structures (i.e., walls or other solid obstructions). Microwaves can be used to transmit across long distances, such as across a city or rural area, without having to run wires or lease private telephone lines. Ultra-Low Frequency radio waves can be used for great distances through the earth or through bodies of water.

Wireless applications might include:

Local Area Network: An existing school is retrofitted with a radio transmitted LAN that connects computers in each classroom to create a common network.

Extended LAN: Multiple schools in a district are connected together by the use of point-to-point microwave transmissions.

Mobile Computing: Laptops are outfitted with modems that use cell telephone technology to dial-in to the central system to join that network as needed.

Network Interface Card

Network interface cards (NIC) act as the physical interface or connection between the computer and the network cable. NICs are installed in an expansion slot in each computer and server on the network, then cables are used to connect the PCs to other devices—other PCs, hubs, routers, etc.—to form a network. A NIC can also be built onto a motherboard, as is the case on a JACE-4/5.

Each NIC has a 6-byte address (called the Media Access Control or MAC address). The first three bytes of the address are the manufacturer's code and the last three bytes are a serial number. The combination makes the address unique, world-wide. The MAC address is used to pass data to and from the computer.

Connectors

As discussed earlier, there is a variety of different types of networking cables and there are various ways to connect them. To select the appropriate interface card for a network, determine the type of cabling and connectors required to support the connection. Keep in mind that some NICs come with more than one interface connector, which can be selected by either jumper or software setting.

Table 1-2 Connector types.

	T-connector, used with 10Base2 networks.
	RJ-11 (4-pin), RJ-45 (8-pin). RJ-45 connectors are used with 10BaseT and 100BaseT networks.
	BNC. BNC connectors are used with 10Base2 networks.
	D-shell
	Fiber, used with 10BaseFL networks.

The OSI Model and the IEEE 802 Standards

Every discussion of network communications includes a discussion of the ISO Open Systems Interconnection (OSI) model. The reason that this model is so important is that it provides a complete model of the functions of a communications system so that different vendors, if they build components that conform to the model, should be able to intercommunicate.

The OSI Model

In 1978, the International Standards Organization (ISO) released specifications that describe a network architecture for connecting dissimilar devices. The specification applied rules to systems so that they would use the same protocol and standards to exchange information.

In 1984, the ISO revised the specification and called it the Open Systems Interconnection (OSI) reference model. The 1984 revision has become an internationally accepted standard for networking—the OSI model has become the best known and most widely used guide to describe networking environments. Vendors design network products based on the specification of the OSI model, which provides a description of how network hardware and software work together in a layered fashion to make network communications possible.

Layered Architecture

The OSI model is an architecture that divides network communications into seven layers. Each layer applies to different network activities, equipment, or protocols. Control is passed from one layer to the next, starting at the application layer in one

station, handed down to the lower layers in the stack for actual transport processing, over the channel to the next station, then handed up the stack to the appropriate application in the receiving station.

Table 1-3 OSI layers.

Layer	Name	Basic Function
7	Application	Defines the language and syntax that programs use to communicate with each other. Common functions at this layer include file open, file close, read and write, and file transfer.
6	Presentation	Translates data into a format that is understood by the receiving computer. For example, this layer might convert BCD to binary. This layer is also used for encryption and decryption.
5	Session	Establishes and manages transmissions between stations, synchronizes transmissions, and handles errors from higher levels. It is the session layer that makes sure the previous request has been fulfilled before the next one is sent.
4	Transport	This layer is responsible for overall end to end validity and integrity of the transmission. It ensures that if a 12MB file is sent, the full 12MB file is received.
3	Network	Determines the best path to specific network destinations and routes data along that path.
2	Data Link	Is responsible for delivering data packets from one node to another - ensuring that the bits that are received are the same bits that were sent. Due to the significant level of detail needed to define node-to-node communications, the IEEE 802 standards committee recently divided the data link layer into two sub-layers: the logical link layer (LLC) and the media access layer (MAC). The logical link layer supports flow control and the MAC layer provides access and error control.
1	Physical	Passes bits onto and receives them from the physical connecting medium. This layer has no understanding of the meaning of the bits, it simply deals with the electrical and mechanical characteristics of the signals and signaling methods.

The IEEE 802 Standards

The IEEE 802 standards, or Project 802, is a set of network standards developed by the IEEE that define network standards for the physical components of a network. These standards have several areas of responsibility including:

- Network interface cards
- Wide area network components
- Components used to create twisted pair and coaxial cable networks

The 802 specification defines the way network interface cards access and transfer data over physical media including connecting, maintaining, and disconnecting network devices. IEEE 802 categories are listed in [Table 1-4](#).

Table 1-4 IEEE 802 categories.

Number	Description
802.1	Covers network management and internetworking.
802.2	Logical Link Control (LLC). Specifies the data link layer for the media access control (MAC) layers defined in 802.3 to 802.5.

Table 1-4 IEEE 802 categories.

Number	Description
802.3	Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet.
802.3U	CSMA/CD Fast Ethernet
802.3Z	CSMA/CD Gigabit Ethernet
802.4	Token Bus LAN.
802.5	Token Ring LAN.
802.6	Metropolitan Area Network (MAN).
802.7	Broadband Technical Advisory Group
802.8	Fiber Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority Access LAN

Drivers

Network drivers provide communication between a network interface card and the network redirector running in the computer. The redirector is part of the networking software that accepts I/O requests for remote files and sends, or redirects, them over the network to another computer. The network administrator uses a setup program to install the driver. During installation, the driver is stored on the computer's hard disk.

NIC drivers reside in the MAC sub-layer of the data link layer of the OSI Model. The MAC sub-layer is responsible for providing shared access for the computer's network interface cards to the physical layer. The NIC driver ensures direct communication between the computer and the NIC, which in turn provides a link between the computer and the rest of the network.

It is common for NIC vendors to provide drivers to the network operating system (NOS) software vendor so that the driver can be included with the NOS.

Protocols

Computers on a network must use an agreed-upon format for transmitting data between the two devices. Generally, a network protocol defines:

- The type of error checking to be used.
- Data compression method, if any.
- How the sending device indicates that it has finished sending a message.
- How the receiving device indicates that it has received a message.

Protocols are typically created by vendors and networking standards organizations. Once established, hardware and software vendors implement them into their products. There is a variety of standard protocols each one has particular advantages and disadvantages. For instance, some are simpler than others, some are more reliable, and some are faster.

From the point of view of the user, the only interesting aspect about protocols is that your computer or device must support the right ones if you want to communicate with other computers. Protocols can be implemented either in hardware or in software.

How Protocols Work

At the transmitting computer, the protocol breaks the data down into small segments called packets. Packets are necessary so that when a computer attempts to transmit a large amount of data, other computers do not transmit until the entire transmission is completed. By breaking data down into smaller segments, individual data transmissions are quicker, allowing more computers the opportunity to transmit. Protocols are also responsible for adding the address of the destination computer and preparing the data for transmission through the NIC onto the data transmission media.

At the destination computer, the protocol is responsible for collecting the packets, stripping off transmitting information, and copying just the data portion of the message to a memory buffer. Then it is responsible for reassembling the data portions of the packets in the correct order and checking the data for errors.

Protocols and the OSI Model

In the OSI architecture, several protocols must work together to ensure that the data is prepared, transferred, received, and acted upon. The work of the various protocols must be coordinated so that there are no conflicts or incomplete operations. This coordination of efforts is referred to as layering.

Protocol Stacks

A protocol stack is a combination of protocols. Each layer specifies a different protocol for handling a function or subsystem of the communication process. Each layer has its own set of rules.

- The application layer initiates or accepts a request.
- The presentation layer adds formatting, display, and encryption information to the packet.
- The session layer adds traffic flow information, which allows stations to determine when a packet is sent.
- The transport layer adds error-handling information.
- The network layer adds sequencing and address information to the packet.
- The data link layer adds error-checking information and prepares data to be placed onto the data transmission media.
- The physical layer sends the packet as a bit stream.

Protocol Bindings

Multiple protocols can be bound to the same network card. When more than one protocol is bound to a particular adapter, the binding order becomes important. The order in which protocols are bound determines the order in which the protocols are used to attempt a successful connection.

In Windows NT, protocol bindings are made in the NT Control Panel. In the Network folder, you can view and modify connections between the NIC cards, protocols, and services that are installed on your computer.

Access Methods

In communications systems in which more than one transmitter has access to the same communication channel, a standard procedure must be established to prevent or handle instances where multiple transmitters attempt to send messages on the media at the same time. Different methods exist to control access to a network.

Contention Methods

Computers transmit data on a first-come, first-served basis. This can lead to a situation where two or more computers transmit simultaneously, which results in a collision. Collisions are detected by monitoring voltage levels on the wire. A voltage level of two or more times higher than expected indicates a collision, since this means there are multiple signals traveling along the backbone at the same time.

In an attempt to prevent this from happening, a contention-based protocol was developed called carrier sense, multiple access (CSMA). A carrier is the presence of any data transmission. CSMA operates like a two-way radio system—a computer with a message to send listens to the network and if it does not hear the carrier signal of another network device, the computer broadcasts its message. Since two devices could theoretically listen, then transmit at the same time, thereby causing a collision, various schemes have been developed to help detect and avoid collisions. The most common methods are as follows:

CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)—

When transmitting devices detect a collision on the network, they each wait a random length of time before attempting to retransmit. The slim chance that both devices will wait the exact same time almost assures that the next attempt will be successful. This is the contention method used in Ethernet networks.

CSMA/CA (Carrier Sense, Multiple Access with Collision Avoidance)—

With collision avoidance, devices announce their intent to transmit. If the announcement causes a collision, the offending station waits a pre-determined period, then retries. This is the contention method used in wireless networks.

Token Passing

Another access method used with a ring topology is token passing. With token passing, network devices pass a token (a special sequence of bits) that grants the device holding it permission to transmit a frame packet. If a station does not need to transmit, it passes the token onto the next station on the network. If a station does have data to transmit, it holds the token and transmits its data to the next station on

the network, which in turn passes it on to the next, and so on. Eventually, the frame returns to the (original) transmitting station. At that point, the source station compares the received frame to that which it transmitted. If the transmission is identical (free of errors), the station releases the token. This is the access method used in Token Ring networks.

Polling

Polling is also referred to as demand priority messaging. With polling, a host device controls which of a collection of secondary devices has access to the communications channel. The primary device checks each secondary device it turn to see if it has anything to transmit. If so, the secondary device is allowed to transmit for a limited period before the primary device continues polling. The primary device can give priority to certain devices, if necessary. Polling is typically used in hierarchical network designs, where there is centralized control of network communications. This is the access method used in RS-485 master/slave networks.

Expanding Networks

Devices that are used to extend transmission distances in networks, therefore expanding their physical reach and/or capacity include repeaters, bridges, and routers. These devices can be used to connect otherwise independent wiring segments, sub-networks, or complete LANs.

Repeaters

Because of attenuation (loss of signal strength), each of the various types of transmission media used in networks has a maximum suggested length. Repeaters can be used to extend the network beyond this distance. Hubs are actually multi-port repeaters.

Repeaters are not simply amplifiers. If repeaters just amplified a signal, they would amplify any electrical noise on the transmission medium as well as the signal. Instead, repeaters analyze signals, make a crisp and clean copy of the data, then pass it onto the next segment of network cable. Although the number of repeaters that you are allowed to use is limited, you can use repeaters to extend the distance of a network well beyond the normal limitations of the transmission medium. Repeaters are used to tie two LANs of the same type together (i.e., Ethernet to Ethernet, Token Ring to Token Ring, etc.).

Advantages of repeaters:

- Repeaters are inexpensive.
- Repeaters extend the distance of a network.
- Since repeaters perform little or no processing, they are very fast.
- Repeaters can connect different types of media such as twisted pair to fiber.

Disadvantages of Repeaters

- Repeaters cannot control network traffic.
- Repeaters cannot filter problems or traffic congestion from other segments.
- After network traffic passes through a number of repeaters, eventually synchronization is lost.

Bridges

The function of a bridge is to connect separate networks together, as well as manage traffic among segments of a LAN. Bridges examine the source and destination addresses of data and they use this information to determine which transmissions should be allowed to pass to another network segment. Traffic whose destination is on the same segment as the sender is confined to that segment. Only inter-network traffic is allowed to pass through the bridge. This is very useful for restricting traffic flow across network segments. Bridges are often used to join two LANs that are already fully expanded.

Bridges know which nodes are on which segments by referring to a filtering database. Some bridges require that a system administrator manually enter address information in this database, but most modern bridges are capable of learning where a node exists. Learning bridges build their own routing tables by examining network traffic and figuring out on which segment a node exists.

Advantages of bridges:

- Bridges can restrict the flow of unnecessary traffic across segments.
- Bridges can resynchronize signals.
- Bridges add reliability to a network.
- Bridged LANs minimize the impact of failures.
- Bridges can segment large LANs into smaller ones to reduce the potential for a catastrophic event that impacts the entire network.

Disadvantages of bridges:

- Bridges are more complex than repeaters.
- Bridges are typically more expensive than repeaters.
- Since they examine all network traffic, bridges are generally much slower than repeaters and might be a potential bottleneck.

Routers

Routers do not simply forward data packets according to Ethernet address as bridges do. Instead, they extract data from the packet and use protocol information in the packet to move data through the network along the most expedient route to its destination. Routers also divide networks logically instead of physically—an IP router can divide a network up into separate subnets so that only traffic destined for particular IP addresses can pass between segments. With all of this processing, routers take more time to process packets than do bridges, but in more complex networks, overall efficiency is improved.

Static routers require an administrator to manually configure a routing table stored in the device that contains the current network topology, whereas dynamic routers discover network topology much like learning bridges. Dynamic routers examine information from other routers and make packet-by-packet decisions about how to send data across the network.

Advantages of routers:

- Routers can choose the best path through a network when there are multiple paths to a destination.

- Routers can isolate problems—they keep problematic messaging from being propagated to the other networks.
- Routers can connect networks that use different media access methods (i.e., protocols).

Disadvantages of routers:

- Routers can create potential bottlenecks in networks.
- Routers are generally more complex and expensive than bridges and repeaters.
- Certain protocols are not routable.

Brouters

Brouters are hybrids of both a bridge and a router. The device functions like a router, relaying data transmissions between networks, until it encounters a data packet that uses a protocol with which it is unfamiliar. Then, it functions as a bridge would.

Advantages of brouters:

- Brouters combine the data-handling capabilities of a router with the protocol transparency of a bridge.

Disadvantages of brouters:

- Brouters are generally more complex and expensive than other internetworking devices.

Gateways

Gateways perform protocol conversion between different types of networks or applications. For instance, a gateway can be used to convert a TCP/IP data packet to NetWare IPX. Gateways perform complete conversion from one protocol to another rather than simply support one protocol from within another, such as IP tunneling. To do this, gateways take data transmissions, strip off their original protocol stack, and repackage them in the protocol stack of the destination network.

Advantages of gateways:

- Gateways can provide internetworking support for drastically different kinds of networks.

Disadvantages of gateways:

- Gateways often produce compromises in speed, efficiency, and cost.
- Gateways are often specialized to a given task (i.e., file transfer).
- Gateways can be network bottlenecks due to the time it takes to translate between protocols.

Networking using IP

In this next section, we focus on how things connect on a network using the Internet Protocol (IP). These are the subtopics:

- [What is IP?](#)—gives an overview of the IP protocol.
- [IP Addressing](#)—talks about IP addresses, subnet masks, and IP address classes.

- [IP Address Allocation](#)—discusses how addresses are allocated, and technologies such as private addressing and network address translation.
- [Associating IP Addresses with Host Names](#)—discusses name resolution techniques including HOSTS files, DNS, DDNS, and WINS.
- [Proxy Servers and Firewalls](#)—talks about these special devices on an IP network. Also included is a review of TCP/IP ports.

What is IP?

The Internet originated as a means of interconnecting computers between universities that were doing research for the Department of Defense. It has a number of communication standards that include:

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML)

IP is one of the standard protocols for sending data on the Internet. It is responsible for addressing and routing of packets between the source and destination computers (called [hosts](#)). Additionally, IP determines if the data is destined for a local or a remote network and then routes the data appropriately.

IP is sometimes referred to as a connectionless protocol because it has no concept of a sequence. Each bit of data is contained in a packet which has no knowledge of other packets. Therefore, it is an unreliable protocol and must be teamed with another protocol (such as TCP) to increase reliability. TCP preserves the sequence of messages sent on the same connection to ensure reconstruction of the message.

IP has gone through several versions since it was originally developed. The current standard is version 4 (written as IPv4), though IPv6 has been ratified and will gradually replace IPv4. This document focuses on IPv4 since that is the current standard.

The OSI Model and TCP/IP

The following discussion uses the OSI model (see [“The OSI Model and the IEEE 802 Standards”](#)) as it relates to native TCP/IP protocol.

Application Layer

This is the top layer of the protocol stack. It includes network software that directly serves the user, providing such things as user interface and application features. The application layer is usually made public through Application Programming Interfaces (API) provided by the vendor. This layer does not actually include application software, but it does enable commercial software to use network services.

TCP/IP includes several application layer protocols for mail, file transfer, remote access, authentication, and name resolution. FTP (File Transfer Protocol) programs are widely used to copy files across a network. All TCP/IP based mail programs use SMTP (Simple Mail Transfer Protocol) to send e-mail. Telnet is a terminal emulator

that provides access to a remote host. And, DNS (Domain Name System) and WINS (Windows Internet Name System) servers resolve names into actual IP addresses, which are required to identify resources on TCP/IP networks.

Presentation and Session Layers

Layers 6 and 5 of the OSI model are not formally defined in TCP/IP. The services are indeed performed, if needed, in other layers of the TCP/IP stack.

Transport Layer

TCP establishes a virtual connection between two stations before they transmit data. Once the connection is established, both sides negotiate the maximum size of a data packet. Although TCP supports packet sizes up to 64KB, in most cases the actual packet size is determined by the underlying network (i.e., Ethernet, which supports a maximum frame size of 1518 bytes). TCP attaches a header to the packet that contains the source and destination ports as well as a sequence number, then it hands the packet over to the network layer (IP).

TCP uses a sliding window system that adjusts the number of packets to be received before an acknowledgement is sent based on network traffic. This flow control mechanism is a real-time means of reducing transmission errors resulting from excessive collisions.

Network Layer

The IP protocol, running on the network layer, accepts data packets from TCP (or UDP) above it and prepares them for the data link protocol layer below. IP converts the IP address of the target station into a physical station address (MAC address) and fragments the packets (if needed) into the required frame size. IP uses the ARP (Address Resolution Protocol) to broadcast the request onto the network, which causes the target station to respond with its MAC address. IP then outputs the packets (called datagrams) and hands them over to the data link layer below it along with the MAC address of the target station or router.

Data Link Layer

Ethernet is the most widely used data link layer protocol. It receives the datagram from the network layer above it and wraps it in its own frame format, which includes a header with source and destination MAC addresses and a trailer that contains checksum data. Ethernet then broadcasts the frame onto the wire using the CSMA/CD (carrier sense multiple access/collision detection) collision avoidance methodology.

Physical Layer

The physical layer specifically addresses the hardware used to transmit data over the network. This includes the voltage used, the timing of data transmission signals, the requirements for establishing the initial communications connection, connectors, and interfaces to data transmission media. This layer provides the electromechanical interface through which data moves among devices on the network. It specifies the

type of data transmission medium used, how that medium interfaces with network devices, and data is encoded into electronic signals for transmission through the medium. Lastly, the physical layer defines what constitutes an acceptable signal.

IP Addressing

What is an IP Address?

In IPv4, an IP address is a 32-bit number which uniquely identifies a host on the Internet. It is typically written in dotted decimal form *nnn.nnn.nnn.nnn* (for example, 192.168.1.1 or 27.34.100.3). An IP address can be thought of as a telephone number for your computer. A telephone number is used to direct calls to your phone. An IP address is used to direct data to your computer (for example, displaying a web page with your browser).

An IP address is assigned to a host by an administrator. It is not hardware specific, but rather is configured through a software interface on each host.

Even though the address is written in the decimal form, the computer reads the address as a series of binary digits consisting of 1s and 0s. When an IP address is represented in dotted decimal form, each set of numbers represents eight bits, called an octet. It takes four octets to make up each 32-bit address. For instance, the dotted-decimal 192.128.23.14 is actually the binary number:

```
11000000.10000000.00010111.00001110
```

The conversion between the binary number (what the computer reads) and what the administrator enters (in dotted decimal form) is illustrated in [Table 1-5](#). Each bit of the octet is a placeholder for a number that is a multiple of two. The multiple for each “on” position in the octet (indicated by a 1) is added together to get the decimal equivalent for the octet. [Table 1-5](#) illustrates this using the 3rd octet from the previous example (00010111).

Table 1-5 Binary to decimal conversion.

Bit	7	6	5	4	3	2	1	0
Multiple of Two	128	64	32	16	8	4	2	1
Example Octet	0	0	0	1	0	1	1	1
Total	16+4+2+1=23							

Therefore, the largest binary number in an octet is 11111111, which is equivalent to 255 (128+64+32+16+8+4+2+1) in decimal form.

IP Classes

An IP address is actually made up of two parts, the network portion and the host portion. The network portion is used to determine whether other IP addresses are on the local network or a remote network. All hosts on a given network share the same network number but must have unique host numbers. Hosts on the same network can communicate with one another without being routed through an IP router. The network portion is analogous to an area code, which is the part of the number which defines a group of telephone users in one area.

For example, in the address 192.168.1.57, the first 3 octets (192.168.1) are the network portion and the last number (57) is the host number. However, this 3-octet boundary is not true for all IP addresses. The boundary changes depending upon which class the address falls into. Classes were designed to accommodate very large to very small networks, as illustrated in [Table 1-6](#).

Table 1-6 Internet addressing class system.

Class	Network Prefix	Network to Host Boundary	Example Network Number	Network Mask	Number of Networks	Number of Hosts on Each Network
A	1-126	N.H.H.H	124.0.0.0	255.0.0.0	126	16,777,216
B	128-191	N.N.H.H	145.10.0.0	255.255.0.0	16,384	65,534
C	192-223	N.N.N.H	192.168.1.0	255.255.255.0	2,097,152	254
D	224-239	Reserved for IP multicasting (a form of broadcasting). See “Special IP Addresses” .				
E	240-247	Reserved for experimental use. See “Special IP Addresses” .				

Network (Subnet) Masks

There is a wide difference between the number of unique hosts on a Class B network (65,534) and a class C network (254). What if you wanted to implement 3 networks with 1000 hosts each? It would be wasteful to use a class B network for so few hosts, but a class C is inadequate. Subnetting was developed as a mechanism to break a single larger network into smaller pieces.

As shown in [Table 1-6](#), each class has a default network mask (sometimes referred to as the subnet mask). The network mask is used to define the network portion of the address and indicate whether the network is subnetted. For example, 255.255.255.0 is the network mask for a class C network that has not been subnetted. The mask 255.255.192.0 is an example of a valid mask for a subnetted class B network.



Note

Each host on a TCP/IP network requires a subnet mask even on a single-segment network.

In order to implement a subnet, some bits are borrowed from the host portion of the address to become the subnet number. In the example above, the subnet number 192 indicates that 2 bits (128+64) were stolen from the 3rd octet. Since those bits are dedicated to the network function, only 6 bits can be used for host numbers (providing host numbers 1-63). Consequently, fewer hosts can be defined on any subnet. Additionally, subnetting uses IP addresses less efficiently because some addresses are lost to special functions such as the network and broadcast addresses (see [“Special IP Addresses”](#)).

The following table gives a summary of how many hosts per subnet, and total subnets result when a range of subnet masks are applied to networks of all classes.

Table 1-7 Subnetting for each class.

Class	Number of Subnet Bits	Subnet Mask	Number of Subnets	Hosts per Subnet
A	0 (not subnetted)	255.0.0.0	0	16,777,216
	1	255.128.0.0	2	8,388,606
	2	255.192.0.0	4	4,194,302
	3	255.224.0.0	8	2,097,150
	4	255.240.0.0	16	1,048,574
	5	255.248.0.0	32	524,286
	6	255.252.0.0	64	262,142
	7	255.254.0.0	128	131,070
	8	255.255.0.0	256	65,534
	9	255.255.128.0	512	32,766
	10	255.255.192.0	1,024	16,382
	11	255.255.224.0	2,048	8,190
	12	255.255.240.0	4,096	4,094
	13	255.255.248.0	8,192	2,046
	14	255.255.252.0	16,384	1,022
	15	255.255.254.0	32,768	510
	16	255.255.255.0	65,536	254
	17	255.255.255.128	131,072	126
	18	255.255.255.192	262,144	62
	19	255.255.255.224	524,288	30
	20	255.255.255.240	1,048,576	14
	21	255.255.255.248	2,097,152	6
22	255.255.255.252	4,194,304	2	
B	0 (not subnetted)	255.255.0.0	0	65,534
	2	255.255.192.0	4	16,382
	3	255.255.224.0	8	8,190
	4	255.255.240.0	16	4,094
	5	255.255.248.0	32	2,046
	6	255.255.252.0	64	1,022
	7	255.255.254.0	128	510
	8	255.255.255.0	256	254
	9	255.255.255.128	512	126
	10	255.255.255.192	1024	62
	11	255.255.255.224	2048	30
	12	255.255.255.240	4096	14
	13	255.255.255.248	8192	6
	14	255.255.255.252	16384	2

Table 1-7 Subnetting for each class.

Class	Number of Subnet Bits	Subnet Mask	Number of Subnets	Hosts per Subnet
C	0 (not subnetted)	255.255.255.0	0	254
	2	255.255.255.192	4	62
	3	255.255.255.224	8	30
	4	255.255.255.240	16	14
	5	255.255.255.248	32	6
	6	255.255.255.252	64	2

In some installations, either the last subnet, or the first and last subnet are unavailable. Whether these subnets are usable depends on the routing protocols in use on the network and the IP implementation on the routing devices on the network.

See [Figure 1-4](#) for examples of subnetted networks.

Special IP Addresses

There are a number of IP addresses (and ranges) that have been reserved for special use. [Table 1-8](#) provides the addresses and a description of the function they serve.

Table 1-8 Special IP addresses.

Address or Range	Function
Addresses ending in 0	This is used to indicate the network ID. For example, 192.168.24.0 would indicate a whole class C network spanning from 192.168.24.1 to 192.168.24.254. Similarly, 125.0.0.0 would indicate an entire class A network from 125.0.0.1 to 125.255.255.255. Never assign an address ending in 0 as a host address.
Addresses ending in 255	An address ending with 255 is a broadcast address. Any data sent to this address would be picked up by all the machines on the local network. The address 192.168.24.255 is an example of the broadcast address for the 192.168.24.0 class C network. Similarly, the broadcast address for the class A network 125.0.0.0 would be 125.255.255.255. Never assign an address ending in 255 as a host address.
127.0.0.1	This is a logical network used by the local machine to address itself (it is also called the loopback address). A host can be reached from other hosts by the assigned IP address (such as 192.168.1.57) but can be reached from itself using the assigned IP address or the loopback address. The loopback address should never be assigned as a host address.
224.0.0.0 to 239.255.255.255	These addresses belong to class D and are used for multicasting. Multicasting is a form of broadcasting in which only participating hosts receive the broadcast. Never assign an address from this range as a host address.

Table 1-8 Special IP addresses.

240.0.0.0 to 247.255.255.255	These addresses are experimental and should never be assigned as a host address.
10.0.0.0 to 10.255.255.255 172.16.0.0 to 172.31.255.255 192.168.0.0 to 192.168.255.255	See " Private IP Addresses ".

IP Address Allocation

The organization responsible for ensuring the uniqueness of IP numbers is the Internet Corporation for Assigned Names and Numbers (ICANN). It delegates the assignment of the public address space to the Internet Assigned Numbers Authority (IANA), which then distributes it to three Regional Internet Registries (RIRs), located throughout the world. These regional authorities then allocate it further to Local Internet Registries (LIRs). LIRs are also known as Internet service providers or ISPs, and they commonly hold a number of address ranges to lease to customers. However, due to the explosion of growth on the Internet, these public addresses are rapidly being depleted.

Private IP Addresses

The designers of IP anticipated this problem and set aside three blocks of IP addresses for use in private networks. This allows organizations to implement IP addressing without having to apply to an ISP for unique global IP addresses for every host. Because these addresses are blocked by the global Internet routing system (the routers will drop packets from these addresses), the address space can simultaneously be used by many different organizations. However, hosts using these private addresses cannot be reached directly from the Internet (nor can they communicate to the Internet).

[Table 1-9](#) lists the sanctioned private addresses for each class.

Table 1-9 Private address ranges.

Class	Range	Description
A	10.0.0.0 to 10.255.255.255	This provides one network of 16,777,216 hosts.
B	172.16.0.0 to 172.31.255.255	This range provides 16 networks, each with 65,534 hosts.
C	192.168.0.0 to 192.168.255.255	This address range provides 254 networks, each with 254 hosts.

Network Address Translation (NAT)

To overcome the reachability limitation, the use of private addresses is commonly teamed with a technique called Network Address Translation (NAT) to provide access to the Internet by hosts that require it. Typically, some device (such as a router, firewall, or proxy server) has a supply of legitimate addresses and translates between a private address and a public one for a host that needs access to or from the Internet.

**Note**

Some administrators have chosen to implement IP addressing on their private networks using legitimate (such as 205.254.1.0) addresses that have not been assigned to them. They use NAT to translate between the legitimate external address and the illegitimate internal address. Depending on how the Internet connection works, this may cause problems in the event of a failure in the connection. It is always best to use private address ranges instead.

See [Figure 1-4](#) for examples of private networks and routers using NAT to translate between private and public IP addresses.

IP Routing and Default Gateway

As discussed previously, any host on a network can communicate with another host on the same network. But what if the host needs to communicate to host on another network across the company or across the world?

If a host wants to communicate outside its network, the administrator sets a default gateway on the host which is the IP address of a router used for communication with other networks.

The router examines an IP packet from the host and compares the destination address with a table of addresses it holds in memory. If it finds a match, it will forward the packet to the address associated with the table entry. This address could be on another network attached directly to the router, or the router could forward it to another router that knows about the network of the destination address.

Routers can build these tables of destinations in a number of different ways. For simple networks, the router could load a table during start-up that was manually created by the administrator. However, more typically, routers use a broadcasting protocol to advertise the networks they know about. Routers use other protocols to discover the shortest path between networks (the least number of hops from router to router). Routes are updated periodically to reflect changes in the availability of a route.

[Figure 1-4](#) illustrates a typical network architecture of routers and default gateways in several networks.

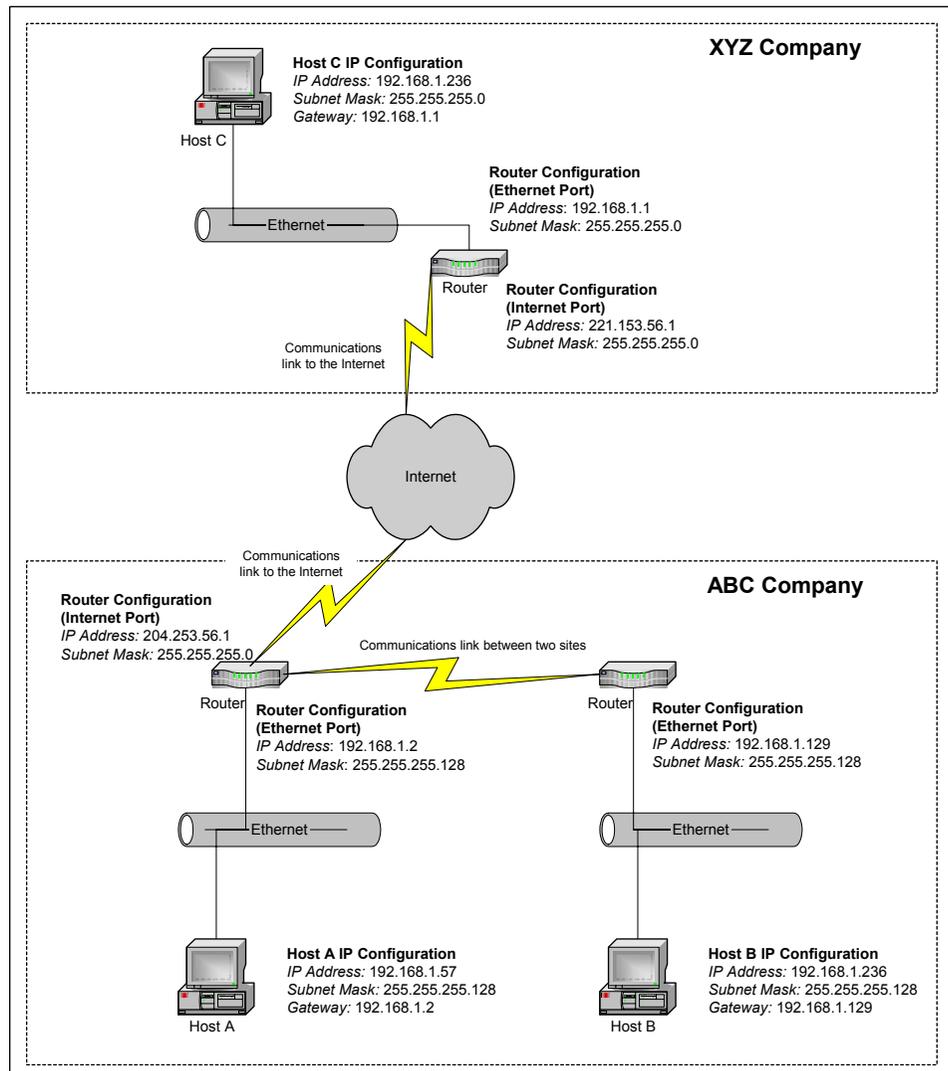
Figure 1-4 Network architecture showing typical IP configurations.

Company XYZ has a single network using the private class C address of 192.168.1.0. The network is not subnetted.

The router is performing NAT to translate the address of Host C to an legitimate address on the external network when Host C uses the Internet.

Company ABC uses the same private class C network, but has subnetted it to provide two networks, one at each site.

The router is performing NAT to translate the addresses of hosts from both private networks to addresses on the external network when the hosts access the Internet.



For information on troubleshooting IP routing and default gateway issues, see the “ping”, “tracert”, and “ipconfig” subtopics of the “Connectivity Troubleshooting Utilities” section on page 2-19.

Static and Dynamic IP Addressing

Once the administrator has decided exactly what IP addressing scheme to implement, she has a number of methods of actually getting the IP address (and subnet mask and default gateway information) onto the host. The simplest method is to configure this information manually on each machine, using the software provided by the operating system. However, this is quite time consuming in a network of more than a few hosts.

Most larger networks are made up of two types of devices: those that need a static (non-changing) IP address because they are accessed frequently by other devices, and most other hosts, which are rarely accessed by others. Hosts that are accessed frequently (like servers and printers) are typically configured manually with a static IP address. The remaining hosts are configured to receive a dynamic address.

Two common protocols used to dynamically assign addresses are BOOTP (Boot Protocol) and DHCP (Dynamic Host Configuration Protocol). There are two components to dynamic addressing: the server and the client.

Servers are set up with a pool of addresses to randomly distribute to clients (the host). They can also provide subnet mask, default gateway information, and DNS server information.

The host is configured to request this information from the server. When the host boots, it sends a broadcast message requesting an IP address, and a server responds with one of the numbers from the pool (and the remaining information). However, the host is not necessarily guaranteed to receive the same IP address every time it boots.

**Note**

DHCP servers can be configured to provide a static IP address to a particular host.

For information on determining DHCP settings for a host, see the “[ipconfig](#)” section on page 2-27.

Associating IP Addresses with Host Names

IP addresses may be easy for computers to work with, but they are hard for humans to remember. This section addresses the technologies used to map the IP addresses assigned to hosts to more friendly names. Once a host has a name, an application running on another host can use the name rather than the IP address to request data.

The HOSTS File

HOSTS files were the original mechanism used to resolve an IP address to a name. The HOSTS file is a text file residing on each local machine. Each line of the text file typically contains an IP address of a host and a name for it.

The primary limitation of this name resolution technique is that the HOSTS file is only usable by the machine on which it resides. For example, you could add an entry to Host A’s HOSTS file mapping Host B’s IP address to a name of “Pluto”. Any application running on Host A could then contact Host B using the name “Pluto”. However, Host B would not be addressable with “Pluto” by other hosts since the mapping only resides in Host A’s local HOSTS file. That means another host wanting to contact “Pluto” would need a similar entry in its local HOSTS file.

Therefore, HOSTS files are difficult to maintain when you have more than a few hosts, and other technologies such as DNS, DDNS and WINS are often used instead.

**Note**

One of the advantages of a HOSTS file is that it is not dependent on a server for name resolution, as is required in the other resolution protocols.

The HOSTS file is always the first place a host looks for name resolution, and if it finds an entry it uses it and does not check other name sources.

DNS

The **domain name system** is the mechanism used by hosts to resolve names on the Internet, and on some private networks as well. Hosts that participate in the DNS system have names like “www.tridium.com”. This is referred to as the **fully qualified domain name**. As with IP addresses, the name is broken down into two parts, the host portion (in this example, “www”) and the domain name (tridium.com). Domain names must also be globally unique so the data intended for that domain gets there and not to some other address. To accomplish this, the domain names are controlled by ICANN, and governed like the IP address system with authority granted to accredited name registrars located throughout the world.

Name Servers

The first level of the domain naming system is organized into classes such as .info, .com, and .org, and countries, such as .uk, and .bm. Top-level domains are then divided into second-level domains such as va.us, co.uk, and tridium.com. A second level domain can then be subdivided into a third level (such as bbc.co.uk) and so forth. Domains can actually be subdivided into 127 levels, but it is rare to see a name with more than 4 levels.

The servers that provide resolution for the naming system are also arranged hierarchically. At the top, there are servers referred to as the root name servers. These servers maintain a table of IP addresses of the first level servers (those serving .com, .org, etc.) The first-level servers know the IP addresses of the name servers for the second level, and the second level servers know the addresses for the third level servers, and so forth. The name servers at the lowest level of the domain name (such as bbc.co.uk) keep track of the IP addresses and names of all the hosts within the domain. Most of the information tracked by these servers is maintained by manually adding entries to the tables.

DNS is one of the largest and busiest distributed database systems in the world. It is probably successful due to two factors: redundancy of servers and caching. At each level there are multiple servers returning queries for their level. In addition, once a name server learns the address of the server for a level (such as .com or co.uk) it caches (stores) that information for faster lookup by another host and to reduce additional queries.

How it Works from the Host

Many host operating systems (OSs) support DNS. Administrators configure the host to look up entries in one or more DNS servers. The host can be configured manually, or it can dynamically receive this setting with DHCP.

When a host tries to contact a particular name (for example, trying to browse www.bbc.co.uk), it first looks in the local HOSTS file, and upon finding no entry, checks with its name server. The name server either returns the information if it knows it, or contacts a root name server, which passes it the address of one of the name servers responsible for the .uk domain. Then that server returns the address of a second-level server handling co.uk, which returns the address of the bbc.co.uk server, which finally returns the IP address for the host named “www”. The browser uses the IP address to fetch the data to open the page.

WINS

WINS is Microsoft’s Windows-only name resolution protocol used by Windows machines prior to Windows 2000. Like DNS, WINS is also implemented with a series of servers that maintain databases of host names to IP addresses. However, setting up WINS is easier than setting up a DNS because WINS actually receives most address records automatically. Administrators name hosts and set one or more WINS server as part of the machine configuration. When a host boots it tells the WINS server its name and current IP address. However, the name that is registered is not in the DNS format of host.domain.xxx, but is in a proprietary format.

WINS is typically used within a company to provide host name resolution of company-specific Windows hosts. It is often teamed with DNS to provide external resolvability.

A pre-Windows 2000 Microsoft host that needs to do a name lookup first looks it up on a WINS server, and if a match is not returned, then the DNS server is checked.

For information on troubleshooting DNS problems on Windows hosts, see the “[nslookup](#)” section on page 2-23.

DDNS

Dynamic DNS (DDNS) is an Internet standard that specifies an automatic method for updating DNS records. This frees the administrator from the time-consuming process of manually updating DNS entries. The server that receives the update must be DDNS compliant.

Microsoft has chosen to replace WINS with DDNS in Windows 2000 computers. With DDNS, the host name that registers on the DDNS server is the FQDN.

In addition, some Internet companies offer a DDNS service for Internet hosts that receive a dynamic IP address from their ISPs. For more information about this topic, see the “[Configuring DDNS on the JACE-4/5](#)” section on page 5-22.

Name lookup from the host follows the rules for DNS.

Proxy Servers and Firewalls

This section discusses these devices and their typical use in IP networks today.

Proxy Server

Proxy servers are usually implemented to provide connection sharing. With connection sharing, an organization can acquire a smaller pool of legitimate IP addresses based on the number of expected simultaneous connections to the Internet rather than the total number of hosts. For example, if an organization has 500 hosts,

but only 250 are expected to be simultaneously connected, the organization can use a private network addressing scheme for the 500 hosts, then lease one legitimate Class C address (providing 254 addresses) for use on the proxy server.

In addition, proxy servers often provide caching, which is a function whereby the server stores the data that is passing through it on its way to the recipient. That way, if another request comes in for the same resource the proxy server (or firewall), can simply fill the request without having to go get the data from its original source. The cache usually has a defined size limit and a storage time limit. So, only the latest or most commonly requested data is typically served up from the cache.

Firewall

A firewall provides network security by restricting access to and/or from the network. A firewall can be a packaged unit sold as a complete firewall solution, or it could be a software package that is loaded on an existing computer situated such that it is the mediator between the network and the Internet.

Firewalls are often implemented to provide users access to and from a secure network via the Internet as well as to separate a company's public Web server from its internal network. Firewalls may also be used to keep separate internal networks secure. For instance, an IS Manager may wish to keep a research or accounting subnet secure from internal snooping.

Firewall protection is often implemented using a combination of the following techniques.

Packet Filter—Also known as a “screening router,” or “static packet filtering”, this technique blocks traffic based on IP address and/or protocol. With address filtering, a packet is filtered based upon the IP address of either the source or the destination address. With protocol filtering, a packet is filtered based upon the protocol being used. In addition, a firewall can limit the availability of a port on a particular host (see [“About Ports”](#)). Once a packet is approved, the client is connected to the destination computer and the firewall no longer monitors the connection.

Static packet filtering is fast because it only checks the header of the packet for the address, protocol and port information. However, it is less secure than other methods because it does not close off the application ports from being scanned.

Stateful Inspection—This technique is also known as “dynamic packet filtering” and tracks a transaction in order to verify that the destination of an inbound packet matches the source of a previous outbound request. In doing so, it opens the packet and examines it for legitimacy.

Typically, stateful inspection is slower than static packet filtering because the firewall:

- checks the entire packet, not just the header information
- monitors the state of the connection
- builds a state table for use in checking future packets on the stream.

However, this technique provides better security because the port is only opened on approved request.

Application proxy—Also known as an “application gateway”, this technique inserts a true barrier between the client computer, which is requesting access to an application, and the application server. The client actually connects to the application gateway which acts on behalf of the client, negotiating with the destination server for information. This, in effect, creates two connections: one between the client and the application gateway and one between the application gateway and the destination server. This effectively hides the internal computers from the view of outside computers.

While this is highly secure, it is slower and consumes more resources than the other firewall technologies.



Note

Working with these devices can be confusing because many devices that are labelled for one function (such as “firewall”) also can provide other functionality as well (such as proxy functions). Therefore, if you encounter an existing device, you should investigate the functions that it provides for the organization.

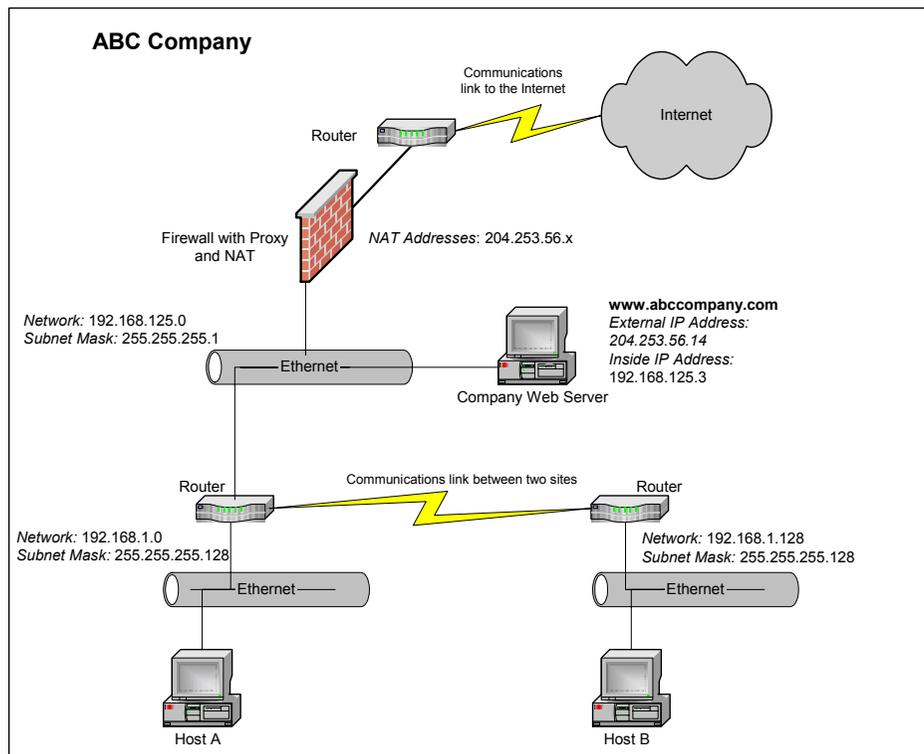
Figure 1-5 shows an typical implementation in Company ABC of a firewall device that has proxy technology built in.

Figure 1-5 Typical implementation of firewall/proxy technologies.

Company ABC has implemented a firewall that also has proxy services and NAT.

The administrator has set up a static mapping of an external IP address for the company web server. In addition, she has set up filtering to only allow the HTTP protocol to that host.

Host A browses a web page on the internet (using HTTP) by securing a dynamically assigned external address from the firewall for the session. The firewall caches the page for later use by Host B. However, the proxy server has another protocol filter which prevents any hosts on an inside network from using the FTP (file transfer) protocol.



For more information on the use of firewalls and proxy servers in the Niagara environment, see “Using a Firewall or Proxy Device,” page 6-4.

About Ports

A port is a communication channel that allows different applications on the same computer to use network resources without interfering with each other. For example, on a multi-function server that runs Telnet, FTP, and web servers, each function uses a different TCP port (typically ports 23, 21, and 80, respectively) for clients to talk to. They are used in TCP/IP networking for long term conversations between two hosts (such as a client accessing a web page on a server).

To go back to the telephone analogy used previously, a port is like a telephone extension in an office environment. While the main telephone number (the IP address) is used to direct a call (the data) to the particular company (the computer), the extension (the port) directs the call to the particular person (the application).

In IP networking, ports can be assigned from 0 to 65535, and many popular applications have default ports, which are assigned or registered by IANA. Many applications (such as Niagara) allow you to change the default port of a particular function (such as the web server). For more information about Niagara ports, see “[Default Niagara Port Numbers](#),” page 6-7.



Note

When the client initiates a conversation with the server it randomly chooses a client-side port (greater than 1024) that is not currently in use. The client uses this port to connect to the server on the server-side port (such as HTTP standard port 80). For examples of this, review the “[netstat](#)” section on page 2-25.

[Table 1-10](#) lists common IP networking functions and their default TCP ports.

Table 1-10 Common well-known TCP ports.

Port	Function
21	FTP (file transfer protocol)
23	Telnet
25	SMTP (simple mail transfer protocol)
37	Time Protocol
53	DNS (domain name service)
80	HTTP (hypertext transfer protocol)
107	Rtelnnet (remote telnet)
110	POP3 (post office protocol version 3)
119	NNTP (network news transfer protocol)
123	NTP (network time protocol)
143	IMAP (Internet message access protocol)
161	SNMP (simple network management protocol)
194	IRC (Internet relay chat protocol)
389	LDAP (lightweight directory access protocol)
401	UPS (uninterruptible power supply)
443	HTTPS (HTTP over TLS/SSL)
447	SNNP (simple network paging protocol)
563	NNTPS (NNTP over TLS/SSL)
636	LDAPS (LDAP over TLS/SSL)

Table 1-10 Common well-known TCP ports.

990	FTPS (FTP over TLS/SSL)
992	Telnet protocol over TLS/SSL
993	IMAP4 protocol over TLS/SSL
994	IRC protocol over TLS/SSL
995	POP3S (POP3 protocol over TLS/SSL)

For a full list of registered and well known ports, see <http://www.iana.org/assignments/port-numbers>.

For a full list of the ports used in a Niagara environment, see the “Default Niagara Port Numbers” section on page 6-7.

Niagara Considerations

This topic provides a review of Niagara hosts, as well as their support for the networking technologies discussed in previous sections. In addition, a summary of the types of communication between Niagara devices is provided.

This information will be used in discussions in subsequent sections.

Niagara Hosts

[Table 1-11](#) provides a summary of the hosts used in a typical network of Niagara devices. Each category of host has different connection methodologies, depending on the function it serves, the operating system used, and the communication ports available.

Table 1-11 Niagara hosts summary.

Category		Current ¹ Hardware Models	Function	Operating System	Primary Communication Port	Selected Secondary Ports ²
Embedded or Full JACE-NP ³	JACE-NP	JACE-NP-1 JACE-NP-2	Controller used to integrate legacy, LonWorks, and BACnet devices. Can also provide GUI interface to Niagara integration.	<ul style="list-style-type: none"> Embedded Windows NT 4.0 Optional: Full version of Windows NT 4.0 Workstation 	10/100 mbit Ethernet with an RJ-45 or BNC connector	Two high-speed RS-232 serial with a DB-9 connector
	JACE-4/5 ⁴	JACE-5	JACE-5x1 JACE-5x2	Controller used to integrate legacy, LonWorks, and BACnet devices.	WindRiver VxWorks	10/100 mbit Ethernet with an RJ-45 connector
		JACE-5x1-UI JACE-5x2-UI	These models can also provide BUI interface to a Niagara integration.			
	JACE-4	JACE-401	Controller used to integrate legacy, BACnet, and direct I/O devices.			

Table 1-11 Niagara hosts summary.

Category	Current ¹ Hardware Models	Function	Operating System	Primary Communication Port	Selected Secondary Ports ²
Engineering PC ⁵	Web Supervisor PC	Server for Niagara integrations. Can also provide GUI interface to Niagara integration. Can also be used to engineer and maintain Niagara integrations.	<ul style="list-style-type: none"> Windows NT 4.0 Windows 2000 	Ethernet	One or more RS-232 serial
	Technician PC	Host used to engineer and maintain integrations but not used as an integration server.			

1. Models of devices that were announced or shipping at the release of this document.
2. Only the ports referenced in later parts of this manual are listed. In some instances, these ports provide alternate communication access to the host. Ports mainly used for control of field devices are not listed.
3. When there is a functional difference between a JACE-NP with Embedded Windows NT 4.0 versus one with a full version of Windows NT 4.0, these hosts may be referred to as “an Embedded JACE-NP or a “Full JACE-NP”.
4. Throughout the remainder of this document the JACE-4 and JACE-5 models may be referred to as JACE-4/5 when they need to be distinguished from JACE-NPs.
5. Since both of these PCs can be used to engineer or maintain a Niagara integration, throughout the remainder of this document these hosts may be referred to as “an engineering PC” when used in the context of setting up or maintaining a Niagara integration.

Available Networking Technologies

Table 1-12 provides a summary of the networking technologies discussed in previous topics and their availability on or for use with Niagara hosts. Most availability is dependent on the operating system of the host.

Table 1-12 Available networking technologies on Niagara hosts.

Technology	JACE-NP	JACE-4/5	Web Supervisor/ Technician PC	Notes
	x= full availability *= limited availability			
Ethernet <ul style="list-style-type: none"> 802.3 Other 	x	x	x	Required for Niagara hosts for configuration.
TCP/IP (IPv4) <ul style="list-style-type: none"> IP Address (x.x.x.x) Subnet Mask Default Gateway 	x	x	x	Required for Niagara hosts for configuration.
Public IP Address	x	x	x	Required for any Niagara host that is connected to from the Internet. See the Niagara Considerations sections in Chapter 3, “Connecting on a LAN” , and Chapter 5, “Connecting to an ISP” .
DHCP	*	*	*	While DHCP is available on these hosts, in most Niagara architectures hosts require a static IP address for ease in data passing. For more restrictions in the use of DHCP, see the “Using DHCP” section on page 3-23. For more information on using DHCP on Niagara hosts directly connected to the Internet, see “Niagara Considerations,” page 5-1 in Chapter 5, “Connecting to an ISP” .

Table 1-12 Available networking technologies on Niagara hosts.

Technology	JACE-NP	JACE-4/5	Web Supervisor/ Technician PC	Notes
	x= full availability *= limited availability			
HOSTS file	x	x	x	Because HOSTS files are local to each host, they do not require dependency on a remote server for name resolution. Therefore, they are the recommended method for name resolution for Niagara hosts.
DNS	x		x	See previous note.
WINS	x		x	See HOSTS file note .
DDNS		*	*	DDNS is available for hosts running Windows 2000. See the "Using Niagara in a Microsoft Windows Server Environment" section on page 3-4. In addition, there is limited support for Internet DDNS on the JACE-4/5 connecting through an ISP using DHCP. See the "Configuring DDNS on the JACE-4/5" section on page 5-22.
Network Address Translation	x	x	x	See Niagara Considerations sections throughout manual.
Proxy Servers	*	*	*	See Chapter 6, "Using a Firewall or Proxy Device" .
Firewalls	*	*	*	See Chapter 6, "Using a Firewall or Proxy Device" .

Communication between Niagara Hosts

Table 1-13 provides a summary of the types of communication between Niagara hosts and to other IP-based hosts. Included is the host that initiates each type of communication, and the host that receives it.

Table 1-13 Communication between Niagara hosts.

Communication		Typical Initiating Host (Client)	Receiving Host (Server)	Description
Browser User Interface (BUI)		Any host	Any Niagara host	Connection by any user to a Niagara station using a Web browser. This includes: <ul style="list-style-type: none"> • Connection to a Web Supervisor, JACE-NP, or JACE-4/5 running WebUI services for viewing a GxPage. • Connection to any Niagara host with or without WebUI services for maintaining a station or viewing data.
Station and Host Administration	Java Desktop Environment (JDE) also called Full User Interface (FUI)	Engineering PC	Any Niagara host	Connection from an Engineering PC for the purpose of maintaining a live station.
	Admin Tool	Engineering PC	Any Niagara host	Connection from an Engineering PC for the purpose of changing host configuration, adding users to the host, installation of a station, software or licenses, or database administration.
	NetMeeting RCMD Telnet FTP Hyperterminal	Windows PC or JACE-NP	JACE-NP (Full NT) ¹ JACE-NP (Embedded NT) ² JACE-4/5 ³	Connection from any PC or JACE-NP for the purpose of maintaining a host or the station on it. This connection is made with alternate maintenance tools as described in "Configuration and Troubleshooting Tools," page 2-1.
Archiving	Pushed archiving	Any Niagara host	JACE-NPs and Web Supervisors running the Database service	Connection from the initiating host to send log data to the receiving host's SQL database for long-term storage.
	Polled archiving	JACE-NPs and Web Supervisors running the Database and Poll Archive services	Any Niagara host	Connection from the initiating host to pick up log data from the receiving host to store in an SQL database for long-term storage.
Alarming	Alarm archiving	Any Niagara host with notification set to archive_remote	JACE-NPs and Web Supervisors running the Database service	Communication from the initiating host to send alarms to a host set up as the archive destination.
	E-mail notification	Any Niagara host running the Mail service.	Any SMTP mail server	Connection from a Niagara host for the purpose of sending an exception (alarm or alert) notification or acknowledgement via e-mail.

Table 1-13 Communication between Niagara hosts.

Communication		Typical Initiating Host (Client)	Receiving Host (Server)	Description
Alarming, continued	Remote Printer notification	Any Web Supervisor or JACE-NP	Any networked printer	Connection from the initiating host for the purpose of sending an exception notification or acknowledgement to a printer.
	Alarm Console acknowledgement	Web Supervisor or any engineering PC	A Niagara host with alarming set up to archive local	Connection from the Engineering PC with the Alarm Console to acknowledge the alarm on the receiving host.
Time synchronization		Any Niagara host with the TimeSync service	Any Internet Time Protocol server	Connection from the initiating PC to a time server in order to synchronize the host's time. The server could be a Niagara host providing this function or any other server running the Internet Time Protocol.
Backup subordinate		Supervisor station	Subordinate station	Connection from a Supervisor to a Subordinate to get a local copy of the runtime database of the station.
Global data passing		Any Niagara host	Any Niagara host	Connection from one host to another to exchange real-time data across a network with interstation links.
Station monitor		Any Niagara host	Any Niagara host	A timed ping from any host to the IP address of the remote host for the purpose of network connectivity. Produces a station alarm if the ping fails.

1. RCMD connections supported.
2. NetMeeting connections supported.
3. Telnet, FTP, and Hyperterminal connections supported.

Additional Information

For more information about the topics covered in this overview, consult the sources listed in [Table 1-14](#) and [Table 1-15](#).



Note

As with any web resource, addresses provided are subject to change. If a listed resource is unavailable, try a search for the article or concept using your favorite search engine.

Table 1-14 Sources for more information about covered topics.

Concept	Source
DNS	"DNS and Microsoft Windows NT 4.0", 1996, Microsoft Corporation, available from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnt40/html/dnsnt4.asp
DNS, Subnetting, TCP/IP	Search on these topics at http://compnetworking.about.com
DNS, Routers, TCP/IP	Search on these topics at http://howstuffworks.com

Table 1-14 Sources for more information about covered topics.

Concept	Source
Fundamentals of Networking	“The World of Computer Networking: A Primer”, 1995, Nortel Networks, Limited, available from http://spark.nstu.nsk.su/BayNetworks/Products/Papers/wp/wp-primer.html
	“Networking Tutorials”, 2001, Lantronix, Inc., available from http://www.lantronix.com/learning/tutorials/index.html
Fundamentals of IP addressing and routing	“IP Routing, Parts 1-6”, 2000, Peter Morrissey, available from http://www.networkcomputing.com/netdesign/1122ipr.html
	“Introduction to the Internet Protocols”, 1987, Charles L. Hedrick, Rutgers University, available from http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/
Ports	“TCP and UDP Port Assignments”, Windows 2000 Resource Kit, 2001, Microsoft Corporation, available from http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cnfc/cnfc_por_gdqc.asp
	“Well Known, Registered, and Dynamic and/or Private Ports”, Internet Assigned Numbers Association (IANA), available from http://www.iana.org/assignments/port-numbers
WINS	“Windows Internet Naming Service (WINS): Architecture and Capacity Planning”, 2000, Microsoft Corporation, available from http://www.microsoft.com/ntserver/techresources/commnet/WINS/WINSwp98/WINS01-12.asp

Request For Comment (RFC) documents are used for communicating standards, specifications, and other information about the Internet. RFCs are developed by the Internet Engineering Task Force, considered by the Internet Engineering Steering Group, and disseminated by the Internet Society as international standards. The RFC Editor is responsible for preparing and organizing standards in their final form. You can find the RFCs published at many sites, including: <http://www.rfc-editor.org/> and <http://www.ietf.org/>.

Table 1-15 lists the RFC number applicable to the concepts covered in this section.

Table 1-15 Applicable RFCs.

Concept	Applicable RFC(s)
Broadcasting	919, 922
DHCP and BootP	2131, 2132
Domain names	1033, 1034, 1035
Dynamic DNS	2136
IP Allocation	2050
Internet Protocol	791
Ports	793, 768
Private Address Space	1918
Subnetting	950

Configuration and Troubleshooting Tools

This section discusses the tools you can use to set up networking on Niagara devices and to troubleshoot connectivity issues. It contains the following main topics:

- [Niagara Configuration Tools](#)
- [Connectivity Troubleshooting Utilities](#)
- [Additional Information](#)

Niagara Configuration Tools

When setting up Niagara hosts, there are several tools that you can use for configuration. Some are Niagara-specific, like the [Admin Tool](#) and the [Remote Command Utility](#), and some, like [NetMeeting](#) and [Hyperterminal](#) are Windows-specific. The others ([Telnet](#) and [FTP](#)) are TCP/IP-specific and are available on both Windows and other host operating systems. These tools are discussed in the following sections, in the order they are most frequently used in the Niagara environment.

Admin Tool

The Admin Tool is installed with the Java Desktop Environment (JDE) during the Niagara [Web Supervisor](#) software installation. Among other things, you can use the Admin Tool to change network configuration settings on any Niagara host. It is the most commonly used configuration tool for Niagara devices.

**Note**

Most changes made through the Admin tool require a reboot of the host to take effect. Sometimes the software does not prompt you to reboot, but you should after making any change.

The Admin Tool can be opened from within the JDE, or independent of it. Use the following procedure to open the Admin Tool and access the network configuration settings:

Procedure 2-1 Starting the Admin Tool and accessing network settings.

-
- Step 1** Choose one of the following actions:
- If you do not currently have the JDE open, on the Windows task bar, click **Start** and select **Programs > Niagara version > Admin Tool**.
The Admin Tool opens outside of the JDE. You see a two-pane window.
 - If you already have the JDE open, double-click **Tools** to expand the contents. Double-click **Admin Tool**.
The Admin Tool opens inside the JDE. You see a three-pane window.
- Step 2** If you are using the Admin Tool outside of the JDE, select **File > Open**.
If you are using the Admin Tool inside the JDE, from the menu, select **Admin Tool > File > Open**.
- Step 3** In the **Connect to Host** dialog box, type the IP address or network name of the host (for example: **192.168.255.255** or **JACE54**).
-  **Note** You can only use the host name if the hosts participate in name resolution. The host you are connecting from must be able to look up the named host in a HOSTS table, or a DNS, or WINS server.
-
- Step 4** In the **Logon** dialog box, type the user name and password for the host.
- Step 5** Click **OK**.
The host information is displayed in the right pane of the window.
- Step 6** In the right window pane, click the **Network Settings** tab.
The network configuration settings for the host display in the right pane of the window.
-

For more information on using the Admin Tool, see the “Getting Started with the Admin Tool” section in the *Niagara Quick Start Guide*.

JACE-NP Remote Control Utilities

The remote control utilities discussed in this section supplement the Admin Tool for maintaining JACE-NPs.

NetMeeting

NetMeeting is a collaboration tool available for Windows hosts. It can be used for video and audio conferencing, chat, file transfer, remote desktop sharing, and a number of other uses.

In the Niagara environment it can be used to remotely control the desktop of a embedded JACE-NP to install printers for a notification recipient, or to configure RAS for remote dial-in (see the “[Configuring Direct Dial on the JACE-NP](#)” section on page 4-17).

NetMeeting is set up to run by default on JACE-NPs using Embedded NT. NetMeeting is **not** set up by default on JACE-NPs running the full version of NT. To access the desktop on this model of JACE, attach a keyboard, mouse, and monitor.

You can download the latest version of NetMeeting at <http://www.microsoft.com/windows/netmeeting/>.

**Caution**

Be **very** careful when using NetMeeting to control a JACE. You must log onto the NT desktop of the JACE with administrative privileges, which means you can change all settings. Changes you make could have unexpected consequences, including making the host inoperable.

Use the following procedure to connect a Windows host to a JACE-NP using a NetMeeting session:

Procedure 2-2 Connecting to a JACE-NP with NetMeeting.

- Step 1** Click **Start** on the Windows task bar and select **Programs > Accessories > Communication > NetMeeting**.

NetMeeting opens.



- Step 2** Click the **Place Call** button.

- Step 3** In the **To** field, type the IP address of the JACE-NP.

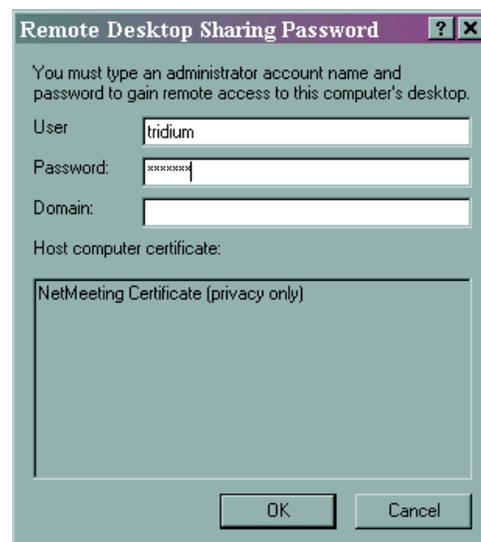
- Step 4** Enable the **Require security for this call** option.

- Step 5** Click **Call**.

The **Remote Desktop Sharing** window opens (see [Figure 2-1](#)).

- Step 6** In the **Remote Desktop Sharing** window, type the host administrator name and password. This is the user used to log in to the JACE via the Admin Tool. You do not need to fill in the **Domain** field.

Figure 2-1 Remote Desktop Sharing window.



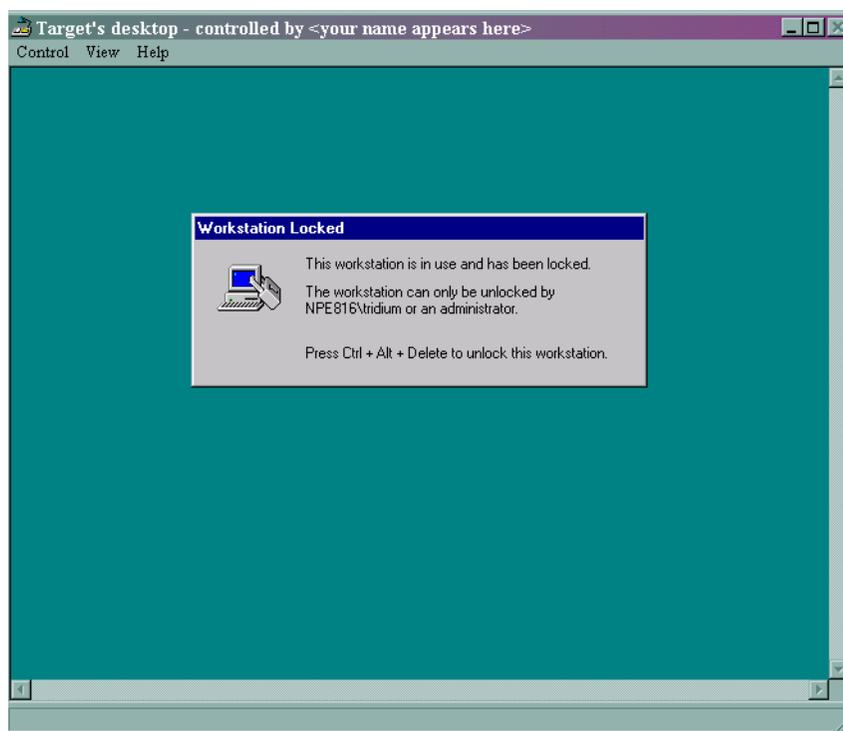


Note For a new JACE-NP, use the initial user name for the administrator account and use the initial password. These are listed on the packing slip which accompanies the unit. For many JACEs the initial user name is **tridium** and the initial password is **niagara**.

Step 7 Click **OK**.

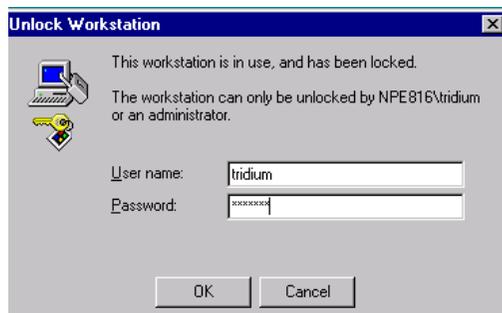
You are connected to the remote JACE-NP with a secure NetMeeting session (see [Figure 2-2](#)). If you see the Windows NT 4.0 desktop, you are finished. Otherwise, continue with the next step to log on to the desktop.

Figure 2-2 Target's Desktop window.



Step 8 From the **Target's Desktop** menu, select **Control > Send Ctrl+Alt+Del**. An **Unlock Workstation** dialog box appears.

Figure 2-3 Unlock Workstation dialog box.



Step 9 Type the host administrator name and password. This is the same name and password with which you log into the Admin Tool.

Step 10 Click **OK**.

The Windows NT 4.0 Desktop appears.

In order to end a NetMeeting session, you cannot close the session window using typical Windows close methods. Use the following procedure to end your NetMeeting session:

Procedure 2-3 Ending a NetMeeting session.

Step 1 From the NetMeeting window menu, select **Control > Send Ctrl+Alt+Del**.

A Windows NT Security dialog box appears.

Step 2 Click the **Logoff** button.

Step 3 Click **OK**.

This logs you off the NT desktop.

Step 4 On the **NetMeeting** program window, click the **End Call** button.



The NetMeeting session to the remote host ends.

Remote Command Utility

Microsoft's Remote Command Utility (RCMD) is the original tool used to access a JACE-NP for the purpose of installing software upgrades and other system maintenance that would otherwise require a monitor, keyboard, and mouse. It can still be used to access any JACE-NP, but is most often used on an NP with the full version of NT.

RCMD has a client and a server component. The server component, RCMD SVC.EXE, runs as a service on the JACE-NP and is enabled on boot. The client component, RCMD.EXE, is a command-line program that you access from the Niagara Console.

When you execute the RCMD command to the JACE-NP you are connected to the JACE-NP at its command prompt and can navigate directories, copy files to and from the host, and execute programs (see [Figure 2-4](#)).

This tool is discussed here, but the following things should be noted:

- The Admin Tool is the preferred tool for most maintenance functions; many tasks formerly performed with RCMD have been added to the [Admin Tool](#).
- Attaching a keyboard, mouse, and monitor is the preferred method of installing software upgrades or performing system maintenance.

**Caution**

Be **very** careful when using RCMD to connect to a JACE. You are logged onto the JACE with administrative privileges, which means you can change many settings. Changes you make could have unexpected consequences, including making the host inoperable.

Use the following procedure to open a RCMD session to a JACE-NP:

Procedure 2-4 Connecting to a JACE-NP with RCMD.

Step 1 Connect to the JACE-NP in one of the following ways:

- Browse the **Network Neighborhood** (in Windows 2000, this is called **My Network Places**) and locate the JACE.
 - Double-click the JACE
 - If requested, log into the JACE using a host user name and password. If instead of being requested for logon information you see the JACE's shared folders, go on to [Step 2](#).
- Open a Niagara Console (see [Step 2](#)).
 - At the command line, type:


```
net use \\<servername>\ipc$ /user:<username>
```

 where
 - *<servername>* is the name of the JACE
 - *<username>* is a host user name on the JACE. If your JACE uses domain security, use */user:<domain>\<username>* instead.
 - When prompted, type the password for the host user name.

You see a confirmation that your command completed successfully.



Note [Step 1](#) supplies the logon credentials that the RCMD program uses to connect to the JACE. After connecting with RCMD you can close the connection you opened in [Step 1](#).

Step 2 If not already open, open a Niagara Console as follows:

- a. Click **Start** on the Windows task bar
- b. Select **Programs > Niagara version > Console**.

The Niagara Console opens.

Step 3 Type:

```
rcmd \\<host name>
```

where **<host name>** is the name of the JACE-NP.

**Tip**

If you do not know the name of the JACE, but do know its IP address, use the [tracert](#) command to determine the name.

Step 4 Press **ENTER**.

RCMD establishes a session between the remote workstation and the JACE. Each command you issue is carried out at the command prompt of the JACE-NP. For an example, see [Figure 2-4](#).

Figure 2-4 RCMD to a JACE-NP with the full version of NT.

```

Niagara Command Line - rcmd \tpubjnpfull
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\niagara\r2.300.315>tpubjnpfull
'tpubjnpfull' is not recognized as an internal or external command,
operable program or batch file.

D:\niagara\r2.300.315>rcmd \\tpubjnpfull
Connected to \\tpubjnpfull

Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\WINNT\system32>d:
D:\>cd \niagara

D:\niagara>dir
Volume in drive D has no label.
Volume Serial Number is 78E4-223E

Directory of D:\niagara

05/26/00  04:51p    <DIR>      .
05/26/00  04:51p    <DIR>      ..
10/09/01  03:12p    <DIR>      rel
03/19/02  02:58p                6,114 Niagara.txt
03/19/02  02:59p                11,552 Niagara2.txt
03/20/02  03:45p    <DIR>      r2.300.315
03/20/02  04:17p    <DIR>      Sysmon
              7 File(s)          17,666 bytes
              2,010,251,264 bytes free
  
```

Step 5 Exit **RCMD** in one of the following ways:

- To exit RCMD but leave the **Console** window open, type: `exit`
- Close the **Console** window.

Hyperterminal

Hyperterminal is a Windows communications utility typically used for [command line](#) access to a variety of hosts (such as switches, routers, and firewalls). It requires either modem access to the device or access via a serial port.

In the Niagara environment, you can use Hyperterminal to directly connect to a JACE-4/5 when you cannot access it remotely across a LAN and need to change settings to make it accessible. You actually connect to the target shell of the [VxWorks OS](#).

About the VxWorks Target Shell

The target shell is a [command-line interpreter](#) for VxWorks. It can be reached using Hyperterminal, or by using the Telnet application over a LAN (see the next section). It allows you to see station output from the JACE-4/5, as well as execute commands.



Caution

Be **very** careful when using the target shell on a JACE-4/5. You log on to the JACE with administrative privileges, which means you can change many settings. Changes you make could have unexpected consequences, including making the JACE inoperable. If possible, use the Admin Tool instead.

Use the following procedure to directly connect to a JACE-4/5 using Hyperterminal.

Procedure 2-5 Connecting to a JACE-4/5 using Hyperterminal.

- Step 1** Based on the model of your controller, choose one of the following procedures to connect the cable between your PC and the controller:

Model	Action
JACE-5	<ol style="list-style-type: none"> a. Attach a null modem cable to a serial port (generally COM1 or COM2) of a Windows NT or 2000 computer. See “About Serial and Null Modem Cables and Adapters,” page 2-12. b. Attach the other end of the cable to serial port 1 of the JACE-5.
JACE-4	<ol style="list-style-type: none"> a. Attach a flat silver satin cable with standard male RJ-45 (8-wire) connectors to the lower RJ-45 port (the RS-232 port) on the JACE-4. b. Connect the other end of the cable to a RJ-45 to DB-9 null modem adapter. See “About Serial and Null Modem Cables and Adapters,” page 2-12. c. Connect the DB-9 adapter to a serial port (generally COM1 or COM2) of a Windows NT or 2000 computer.

The two devices are now physically connected.



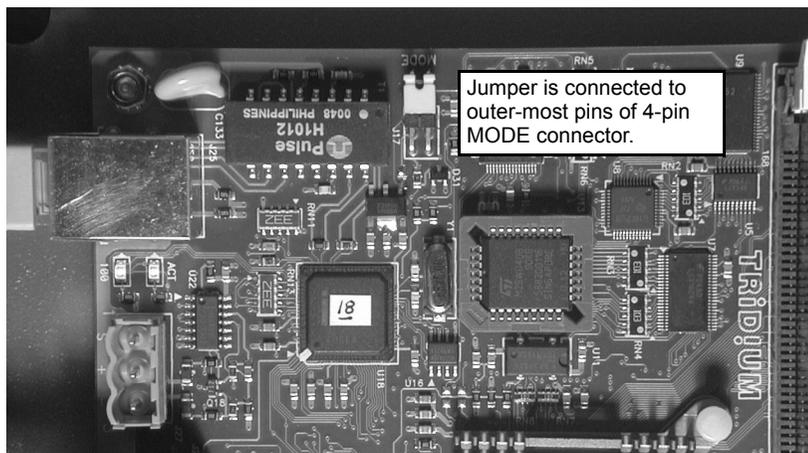
Caution

Connecting to the JACE via the serial port disables communication to any serial device previously using the COM1 port. If you have configured another serial device to use COM1 on the JACE, any driver configured to use that port will receive an error. This is especially relevant for the JACE-4 where the COM ports are software-selectable. If the RS-485 port is configured as COM1 and you attach to the JACE on the RS-232 port, the RS-485 port will not function until you disconnect from the RS-232 port.

- Step 2** Open Hyperterminal as follows:
- On Windows NT—Click **Start** then choose **Programs > Accessories > Hyperterminal > Hyperterminal**
 - On Windows 2000—Click **Start** then choose **Programs > Accessories > Communications > Hyperterminal**
- Step 3** In the **Connection Description** dialog box, type a name for this session. For example:
- ```
Direct connect to JACE
```
- Step 4** Click **OK**.
- Step 5** In the **Connect to** dialog box, choose either COM1 or COM2, depending on which serial port the null modem cable or adapter is attached to on your PC.
- This makes the remaining options on the dialog box unavailable.
- Step 6** Click **OK**.
- Step 7** On the **Comm Properties** dialog box, choose the following settings:
- Bits per Second: **9600**
  - Data bits: **8**
  - Parity: **None**
  - Stop bits: **1**
  - Flow control: **Hardware**
- Step 8** Click **OK**.
- The Hyperterminal session is now set up.
- Step 9** If you are connecting to a JACE-4, open the cover. Otherwise, skip to the next step.
- Step 10** Find the 4-pin connector on the motherboard:
- **On the JACE-4**—the connector is at the top of the board and is marked MODE. On some models of JACE-4, this connector is in the top left quadrant (Figure 2-5), in others, it is in the top right quadrant.
  - **On the JACE-5**—the connector is to the left of RS-232 serial port 1.
- Step 11** Connect a jumper to two pins of the connector:

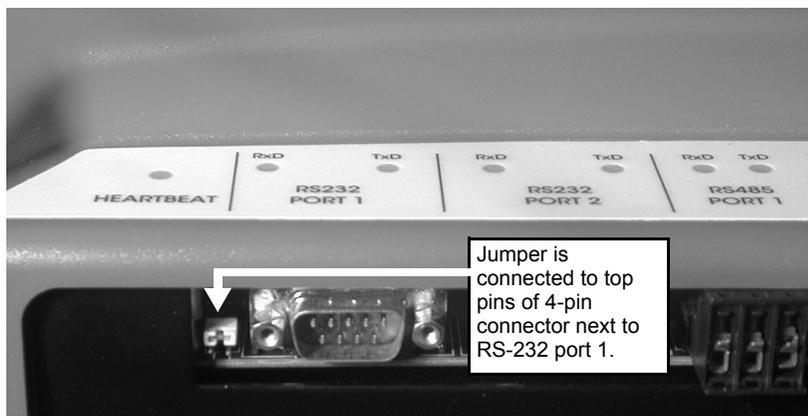
- **On the JACE-4**—connect it to the outer-most two pins (Figure 2-5).

Figure 2-5 4-pin connector with correct jumper position on the JACE-4.



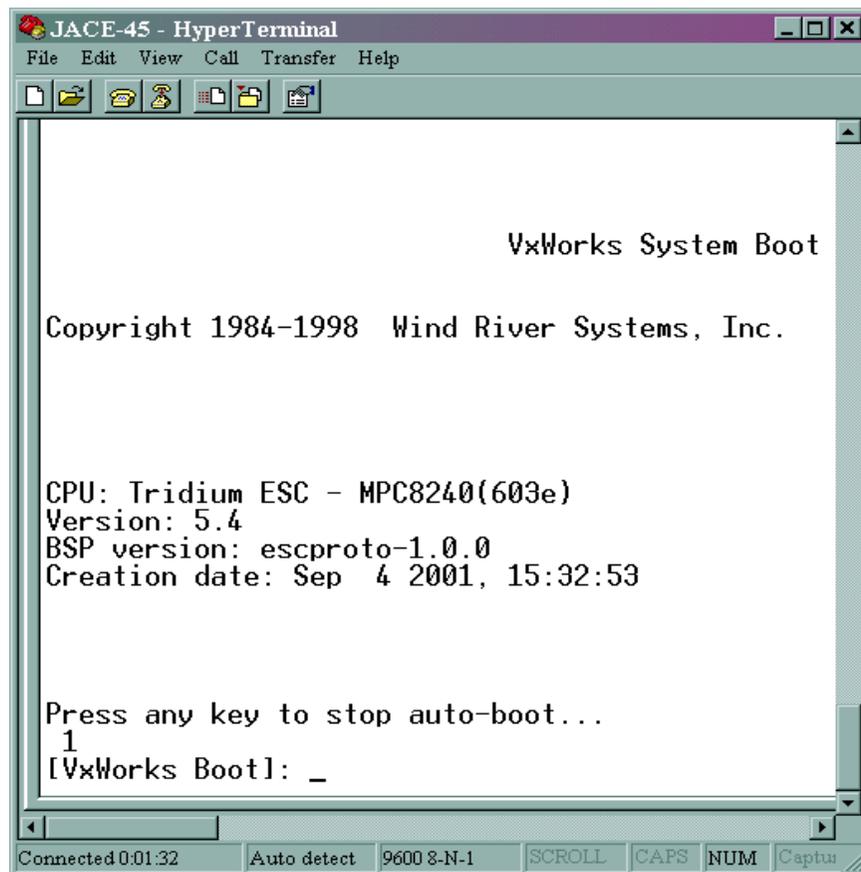
- **On the JACE-5**—connect it to the top two pins (Figure 2-6). If you cannot easily access the connector, remove the plastic and metal covers.

Figure 2-6 4-pin connector with correct jumper position on the JACE-5.



- Step 12** With Hyperterminal open on the Windows PC, unplug the 6-position power connector on the JACE-4/5, then plug it back in.
- Step 13** When you see text appear in the Hyperterminal window, press any key to break out of the boot sequence of the JACE (Figure 2-7).

Figure 2-7 VxWorks boot.



You see a prompt similar to the following:

```
[VxWorks Boot]:
```

You are connected to the target shell and it is ready for command input.

- Step 14** When finished typing commands at the command prompt, follow the next procedure to disconnect from the JACE.

---

#### Procedure 2-6 Disconnecting from the JACE when using Hyperterminal.

---

- Step 1** Press the **Disconnect**  button on the Hyperterminal tool bar.  
Your session is disconnected from the JACE.
- Step 2** Close the application by choosing **File > Exit** to exit the Hyperterminal application.
- Step 3** Remove the jumper from the JACE-4/5.
- Step 4** Reboot the JACE by removing the power connector, waiting for all lights to extinguish, and plugging the power connector back in.
-

## About Serial and Null Modem Cables and Adapters

The standard RS-232C serial communications interface defines a signal protocol used between data terminal equipment (DTE) (such as your engineering PC) and a data communications equipment (DCE) (such as a modem).

The protocol signals are transmitted on a set of lines within the standard serial cable. Two lines (RXD and TXD) are used for sending and receiving data. They provide a full duplex connection between the two devices (the data can be transmitted in both directions simultaneously). Two more lines (CTS and RTS) form a flow control pair that is typically used to throttle the communication flow on the transmit and receive lines. The last pair of lines (DTR and RTS) is typically used for a connection true/false instead of character data flow.

### JACE-5

Since the serial connection on a JACE-5 is DTE, a standard serial cable cannot be used to connect it to the DTE serial port on your PC. When you need to connect two DTE devices together a null modem cable is used instead. A null modem makes the other end of a DTE connection look like a DCE connection.

Standard serial and null modem cables are widely available commercially.

### JACE-4

The serial port on a JACE-4 is also DTE, however the serial connection on the JACE-4 is RJ-45, and not the standard DB-9. It was designed this way because a DB-9 connector does not fit through a standard 1/2-inch knockout hole, and because wiring a RJ-45 connector is easier than wiring a DB-9 connector. In addition, the RJ-45 connector will pass through a conduit fitting so that if conduit is a requirement on the installation, it may not be necessary to cut the terminations off a ready made cable.

The cable used between a JACE-4's serial port and another DTE or DCE device is 8-conductor flat, silver satin stranded cable with the addition of an RJ-45 (female) to DB-9 (female) adapter. Note that silver satin cable is not the standard Ethernet cable, in which the pairs are twisted around each other. When used with the JACE-4, the twisting of the pairs may cause undesirable effects on the serial communication, therefore we recommend the use of flat silver satin cable instead.

Similar to the standard Ethernet twisted pair, however, the silver satin cable should be wired straight through (see the [“About Ethernet Straight Through and Crossover Cables”](#) section on page 3-10). When connecting to a DCE device, the RJ-45 to DB-9 adapter is also pinned straight through.

To connect a JACE-4 to another DTE device, such as your PC, you can use a silver-satin straight-through cable and a null-modem adapter, or wire the silver-satin in a null modem configuration and use a straight through adapter (see [“Wiring a Silver Satin Null Modem Cable,”](#) page 2-14).

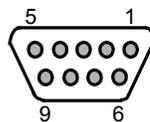
You can either purchase a null modem adapter from us, or use the information in [Table 2-16](#) to assemble the DB-9 to RJ-45 adapter. Do not use a third-party ready-made adapter unless you can verify that it has been pinned out in the manner specified in [Table 2-16](#).

**Table 2-16 DB-9 to RJ-45 adapter pinouts.**

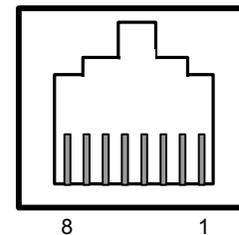
| Type of Adapter                                   | DB-9 Female Pin | Signal                 |                     | RJ-45 Female Pin |
|---------------------------------------------------|-----------------|------------------------|---------------------|------------------|
| Straight-through (for connecting to a DCE device) | 1               | DCD                    | Data carrier detect | 5                |
|                                                   | 2               | RXD                    | Receive data        | 6                |
|                                                   | 3               | TXD                    | Transmit data       | 3                |
|                                                   | 4               | DTR                    | Data terminal ready | 1                |
|                                                   | 5               | GND                    | Ground              | 4                |
|                                                   | 6               | DSR                    | Data set ready      | 8                |
|                                                   | 7               | RTS                    | Request to send     | 2                |
|                                                   | 8               | CTS                    | Clear to send       | 7                |
|                                                   | 9               | not used on the JACE-4 |                     |                  |
| Null Modem (for connecting to another DTE device) | 1               | DCD                    | Data carrier detect | 5                |
|                                                   | 2               | TXD                    | Transmit data       | 3                |
|                                                   | 3               | RXD                    | Receive data        | 6                |
|                                                   | 4               | DSR                    | Data set ready      | 8                |
|                                                   | 5               | GND                    | Ground              | 4                |
|                                                   | 6               | DTR                    | Data terminal ready | 1                |
|                                                   | 7               | CTS                    | Clear to send       | 7                |
|                                                   | 8               | RTS                    | Request to send     | 2                |
|                                                   | 9               | not used on the JACE-4 |                     |                  |

The following figures provide a pin reference for both DB-9 (female) and RJ-45 (female) connectors.

**Figure 2-8 DB-9 female pin reference.**



**Figure 2-9 RJ-45 female pin reference.**



**Note**

If the serial port on your serial device has a DB-25 male connector instead of the DB-9 male, use a standard DB-9 female to DB-25 female adapter (or adapter cable) to make the conversion.

**Wiring a Silver Satin Null Modem Cable**—You can make a null modem cable by attaching the RJ-45 connector upside down on one end, which effectively connects the input signals on one connector to the output signals of the other. However, you should wire pins 4 and 5 straight through, which means you need to actually cross them over in the reversed end (see [Table 2-17](#)).

**Table 2-17 Silver satin null modem cable pinouts.**

| Connector #1 |                | Cable Lines | Connector #2   |           |
|--------------|----------------|-------------|----------------|-----------|
| RJ-45 Pin    | Signal         |             | Signal         | RJ-45 Pin |
| 1            | RTS            | -----       | CTS            | 8         |
| 2            | DTR            | -----       | DSR            | 7         |
| 3            | TXD            | -----       | RXD            | 6         |
| 4            | GND            | -----       | DCD (not used) | 5         |
| 5            | DCD (not used) | -----       | GND            | 4         |
| 6            | RXD            | -----       | TXD            | 3         |
| 7            | DSR            | -----       | DTR            | 2         |
| 8            | CTS            | -----       | RTS            | 1         |

## Telnet

Telnet is terminal emulation utility commonly used in IP networking for command-line access to a variety of hosts.

In the Niagara environment, you can use Telnet to connect to the target shell of a JACE-4/5 over a LAN (see “[About the VxWorks Target Shell](#)”, especially the [Caution](#)). You can then use it to change settings if the Admin Tool is not adequate.

### Enabling Telnet on a JACE-4/5

However, in order to use Telnet, it must first be enabled on the JACE-4/5. This involves editing the system.properties file, which is one of a number of configuration files used by Niagara hosts. Use the following procedure to enable Telnet on the JACE-4/5.



#### Caution

Enabling Telnet on a JACE creates a greater security risk since Telnet is a utility available on most operating systems. There is a greater risk that someone could access the host with Telnet, rather than with our Admin Tool, which has a restricted installation.

#### Procedure 2-7 Enabling Telnet on the JACE-4/5.

- Step 1** Start the Admin Tool (see steps 1—5 of “[Starting the Admin Tool and accessing network settings.](#)”).
- Step 2** From the menu choose **Host > Edit System Properties**.  
The system.properties file opens in a text editor window.
- Step 3** Add a new empty line to the bottom of the file by placing your cursor at the end of the last text line and pressing **ENTER**.

**Step 4** Type:

```
telnetEnable=true
```

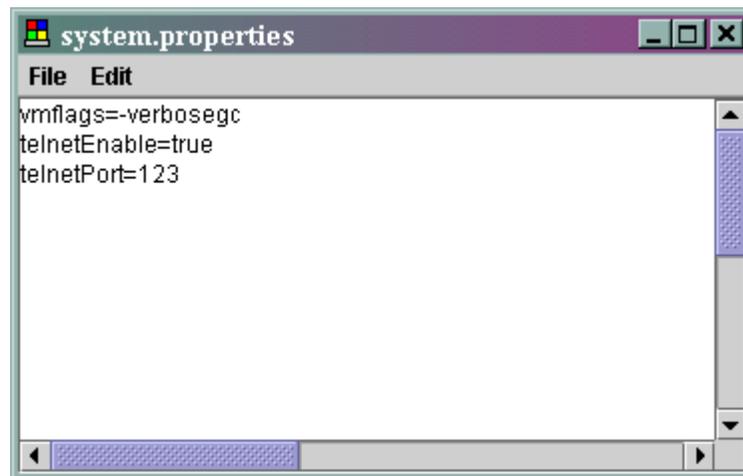
**Step 5** Optionally, if you wish to change the default port for Telnet, add a new empty line and type:

```
telnetPort=xxx
```

where **xxx** is the telnet port on which you want the JACE to respond.

Your system.properties file should look similar to [Figure 2-10](#), if you added both lines.

**Figure 2-10** Sample system.properties file after Telnet additions.



**Step 6** From the system.properties menu, choose **File > Close**.

You are prompted to save any changes you made to the file.

**Step 7** Click **Yes** to save your changes. Otherwise, click **No** to lose your changes. Clicking **Cancel** returns you to the system.properties edit window.

**Step 8** Reboot the JACE.

After booting, the JACE can be reached via Telnet.

## Connecting with Windows Telnet

Use the following procedure to connect via a LAN to a JACE-4/5 using Telnet from a Windows host:

### Procedure 2-8 Connecting to a JACE-4/5 using Windows Telnet.

**Step 1** From the **Start** menu, choose **Run**.

**Step 2** Type:

```
telnet <JACE-4/5> <port>
```

where *<JACE-4/5>* is the name or IP address of the JACE you want to connect to and *<port>* is the port you (optionally) specified in step 5 of the previous procedure.

You are connected to the JACE and see a command prompt similar to the following:

**JACE login:**

- Step 3** Type the name of the host administrator account. This is the user used to log into the JACE via the Admin Tool.
  - Step 4** Press **ENTER**.  
You are prompted for a password.
  - Step 5** Type the password of the host administrator account.
  - Step 6** Press **ENTER**.  
You are logged into the JACE at the command prompt.
  - Step 7** To exit a telnet session, close the **Telnet** window.
- 

## Using Hyperterminal to Telnet

If you are using a Windows 2000 host, you can also use Hyperterminal in telnet mode to connect to a JACE over the LAN. You may prefer to use Hyperterminal for telnetting into a JACE-4/5 because it provides a graphical user interface (GUI).

Follow the next steps to set up a Hyperterminal session for telnet mode:

### Procedure 2-9 Setting up Hyperterminal in Telnet mode (Windows 2000 only).

---

- Step 1** Open Hyperterminal as follows:
  - On Windows NT—Click **Start** then choose **Programs > Accessories > Hyperterminal > Hyperterminal**
  - On Windows 2000—Click **Start** then choose **Programs > Accessories > Communications > Hyperterminal**
- Step 2** In the **Connection Description** dialog box, type a name for this session. For example:  
**Telnet to JACE**
- Step 3** Click **OK**.  
The **Connect to** dialog box opens.
- Step 4** In the **Connect using** field, choose **TCP/IP (Winsock)**
- Step 5** In the **Host address** field, type the name or IP address of the JACE you want to connect to and click **OK**.  
You are connected to the JACE and see a command prompt similar to the following:  
**JACE login:**
- Step 6** Type the name of the host administrator account. This is the user used to log into the JACE via the Admin Tool.

- Step 7** Press **ENTER**.  
You are prompted for a password.
- Step 8** Type the password of the host administrator account.
- Step 9** Press **ENTER**.  
You are logged into the JACE at the command prompt.
- Step 10** When finished typing commands at the command prompt, disconnect from the JACE and close the Hyperterminal window.
- 

## FTP

FTP (the file transfer protocol) is used in IP networking to transfer files to and from a variety of hosts. Many OSs (such as Windows) include an implementation of an FTP client utility. In the Niagara environment, you can use an FTP utility on your PC to transfer files such as HOSTS files and `niagarad.properties` to and from a JACE-4/5.



### Caution

- As with the use of the target shell, using FTP to transfer files to a JACE could result in host or station inoperability if you send a file with incorrect information. The Admin Tool is the preferred method of changing data in these files.
- In addition, enabling FTP on a JACE creates a greater security risk since FTP is a utility available on many operating systems. There is a greater risk that someone could access the host with FTP, rather than with our Admin Tool, which has a restricted installation.

Before you transfer files, however, you must enable the FTP server on the JACE-4/5. Use the following procedure to enable FTP on the JACE.

#### Procedure 2-10 Enabling FTP on the JACE-4/5.

- Step 1** Start the Admin Tool (see steps 1 to 5 of “[Starting the Admin Tool and accessing network settings.](#),” page 2-2).
- Step 2** From the menu choose **Host > Edit System Properties**.  
The `system.properties` file opens in a text editor window.
- Step 3** Add a new empty line to the bottom of the file by placing your cursor at the end of the last text line and pressing **ENTER**.
- Step 4** Type:  
`ftpEnable=true`

Your `system.properties` file should look similar to [Figure 2-11](#).

**Figure 2-11** Sample `system.properties` file after FTP addition.

- Step 5** From the `system.properties` menu, choose **File > Close**.  
You are prompted to save any changes you made to the file.
- Step 6** Click **Yes** to save your changes. Otherwise, click **No** to lose your changes. Clicking **Cancel** returns you to the `system.properties` edit window.
- Step 7** Reboot the JACE.  
After booting, the JACE can be reached via FTP.

---

Use the following procedure to connect via a LAN to a JACE-4/5 using FTP from a Windows host.

---

**Procedure 2-11** Connecting to a JACE-4/5 using FTP.

---

- Step 1** From the **Start** menu, choose **Run**.
- Step 2** Type:  
`ftp <JACE-4/5>`  
where `<JACE-4/5>` is the name or IP address of the JACE you want to connect to.  
You are connected to the JACE and see a command prompt similar to the following:  
`JACE login:`
- Step 3** Type the name of the host administrator account. This is the user used to log into the JACE via the Admin Tool.
- Step 4** Press **ENTER**.  
You are prompted for a password.
- Step 5** Type the password of the host administrator account.
- Step 6** Press **ENTER**.  
You are logged in to the JACE at the `ftp>` prompt.

**Tip**

To see a list of commands, type `help` at the `ftp>` prompt. You can also type `help <command>` to get a description of each command.

Common commands to change directories and transfer files include:

**Table 2-18 Common FTP commands.**

| Command             |                        | Use to...                                                                                                                                          |
|---------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>lcd</code>    | local change directory | change directories on your PC. For example:<br><code>lcd d:\niagara\R2.300.315\emb</code>                                                          |
| <code>cd</code>     | change directory       | change directories on the JACE. For example:<br><code>cd \rel</code><br><code>cd \sm</code>                                                        |
| <code>ls</code>     | list                   | list files in the current directory                                                                                                                |
| <code>dir</code>    | directory              | list files in the current directory with details                                                                                                   |
| <code>binary</code> | binary                 | set the file transfer type to binary<br><br><b>Note:</b> Before transferring files on or off the JACE, be sure to set the transfer type to binary. |
| <code>put</code>    | put                    | copy a single file from the local directory to the current directory on the JACE. For example:<br><code>put port.properties</code>                 |
| <code>get</code>    | get                    | copy a single file from the JACE to the local directory on your PC. For example:<br><code>get port.properties</code>                               |

**Step 7** To log off the host and exit your FTP session, type:

`quit`

**Step 8** Press **ENTER**.

**Step 9** If you made any changes, reboot the JACE to enable them.

## Connectivity Troubleshooting Utilities

There are a number of applications to help you diagnose host connectivity issues. Some are TCP/IP-specific utilities that are available on most operating systems and some can only be run on the Windows operating system. This topic covers the following troubleshooting utilities:

- [ping](#)
- [tracert](#)
- [nslookup](#)
- [netstat](#)
- [ipconfig](#)

These utilities can be used on Niagara hosts that run the Windows OS, but they are not supported on JACE-4/5s.

## Using Windows Command-line Utilities

The versions of these utilities that ship by default with the Windows OS are executed at a [command prompt](#). However, there are many GUI versions freely available for download from the Internet. Examples provided in each subtopic were run at a command prompt of a Windows 2000 host.

### Opening a Command Prompt

Use the following procedure to open a command prompt window on a Windows host:

#### Procedure 2-12 Opening a command prompt window.

**Step 1** Choose one of the following actions based on your OS:

| Operating System          | Action                                                                                                                                                                     |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| for Windows NT 4.0 (full) | Choose <b>Start &gt; Programs &gt; Command Prompt</b> .                                                                                                                    |
| for Embedded NT 4.0       | <ul style="list-style-type: none"> <li>• Choose <b>Start &gt; Run</b>.</li> <li>• At the <b>Open</b> prompt, type <code>cmd</code>.</li> <li>• Click <b>OK</b>.</li> </ul> |
| for Windows 2000          | Choose <b>Start &gt; Programs &gt; Accessories &gt; Command Prompt</b> .                                                                                                   |

A command prompt window opens.

As is true for most programs that execute from a Windows command line, you can receive information about additional program options by typing:

```
<ProgramName> /?
```

where `<ProgramName>` is the name of each utility described in the next section.

## TCP/IP Utilities

### ping

Packet Internet groper (`ping`) is a utility that checks the availability and response time of a network host. It uses the Internet control message protocol (ICMP).

The `ping` utility is typically used to determine whether one host can reach another host. For example, if Host A (Pluto) was having difficulty connecting to Host B (Saturn), an administrator could `ping` the IP address (or name) of Saturn to see if it responds. If the host does not respond, there could be a problem with the host configuration, or the Ethernet connectivity (cable, Ethernet card, hub). If the host responds, but responds slowly, that may indicate other problems more easily diagnosed with the `tracert` utility (see the next section).

The typical use of the ping command for a Windows-based host is:

```
ping <ipaddress>
```

or

```
ping <hostname>
```

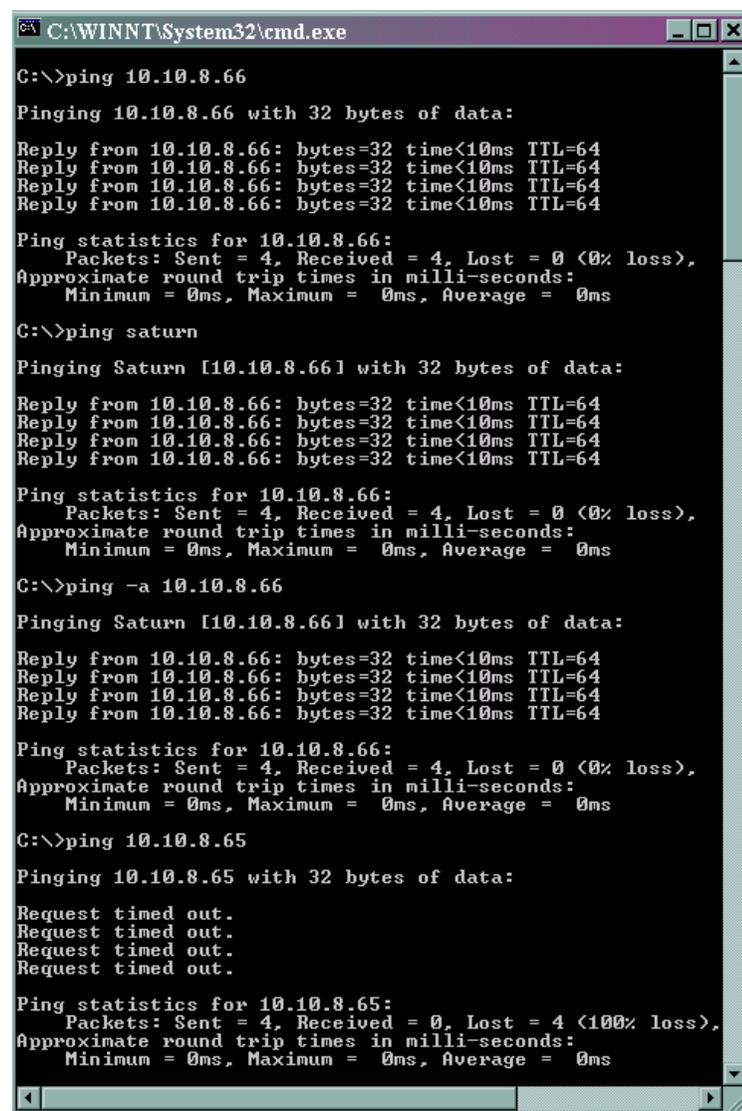
where

<ipaddress> is the IP address of the host to which you want to check connectivity.

<hostname> is the name of the host to which you want to check connectivity.

Figure 2-12 shows several examples of the use of the ping command.

Figure 2-12 Ping utility examples.



```
C:\WINNT\System32\cmd.exe
C:\>ping 10.10.8.66
Pinging 10.10.8.66 with 32 bytes of data:
Reply from 10.10.8.66: bytes=32 time<10ms TTL=64
Ping statistics for 10.10.8.66:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping saturn
Pinging Saturn [10.10.8.66] with 32 bytes of data:
Reply from 10.10.8.66: bytes=32 time<10ms TTL=64
Ping statistics for 10.10.8.66:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping -a 10.10.8.66
Pinging Saturn [10.10.8.66] with 32 bytes of data:
Reply from 10.10.8.66: bytes=32 time<10ms TTL=64
Ping statistics for 10.10.8.66:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.8.65
Pinging 10.10.8.65 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.8.65:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The following things are shown with these examples:

- The ping command was executed 4 different times.

- In the first two examples, a host was pinged using its IP address, then its name.
- In the third example a switch was used (-a) to show the name while pinging by IP address.
- The host responded in under 10 milliseconds in each of the above instances, showing good connectivity.
- The fourth examples shows the response you see when an IP address is not responding.

**Note**


---

The ICMP protocol can be blocked (filtered) by routers and firewalls. That means if you ping a host that is located on the other side of a blocking device, you will see the “Request timed out” message rather than a “Reply” message, even if the host is available.

---

**tracert**

The **tracert** (tracert) utility shows the path taken by an IP packet between the source and the destination address. It is also an ICMP-based protocol, so it is subject to the filtering restrictions mentioned in the previous note.

For example, if the host Saturn failed to reply with the ping command (or replied slowly), the administrator could use **tracert** to trace the path of the communication between the two hosts to determine where the communication fault lay.

Typical use for the tracert command for a Windows-based host is:

```
tracert <ipaddress>
```

or

```
tracert <hostname>
```

where

<ipaddress> is the IP address of the host you want to check connectivity to.

<hostname> is the name of the host you want to check connectivity to.

**Note**


---

On most other operating systems, the command is typed “tracert”, but the Windows command is typed “tracert”.

---

[Figure 2-13](#) shows an example of a traceroute to the host [www.bbs.co.uk](http://www.bbs.co.uk).

Figure 2-13 Tracert utility example.

```

C:\WINNT\System32\cmd.exe
C:\>tracert www.bbs.co.uk

Tracing route to www.bbs.co.uk [213.48.95.8]
over a maximum of 30 hops:

 1 <10 ms <10 ms <10 ms 10.10.8.1
 2 10 ms 10 ms <10 ms $4-1-5-0.Q-RTR1.RICH.verizon-gni.net [209.158.215.49]
 3 10 ms 10 ms 10 ms wdc-edge-05.inet.qwest.net [205.171.34.33]
 4 10 ms 20 ms 10 ms wdc-core-01.inet.qwest.net [205.171.24.81]
 5 10 ms 10 ms 10 ms wdc-brdr-03.inet.qwest.net [205.171.24.38]
 6 10 ms 10 ms 20 ms acr1-sonet7-0-1-0.Washington.cw.net [206.24.227.233]
 7 40 ms 10 ms 20 ms agr3-loopback.Washington.cw.net [206.24.226.103]
 8 10 ms 10 ms 30 ms dcr2-so-6-2-0.Washington.cw.net [206.24.238.185]
 9 80 ms 91 ms 90 ms bcr2.Thameside.cw.net [166.63.210.62]
 10 90 ms 90 ms 90 ms zcr1-so-1-0-0.LondonInt.cw.net [166.63.209.198]
 11 90 ms 80 ms 90 ms telewest.LondonInt.cw.net [166.63.222.38]
 12 110 ms 100 ms 110 ms h31-isp1-kno.cableinet.net [193.38.108.74]
 13 110 ms 110 ms 110 ms 194.117.156.160
 14 110 ms 111 ms 110 ms 213.48.95.8

Trace complete.

C:\>

```

The following things can be noted about this traceroute:

- The traceroute lists the IP address for the host (213.48.95.8).
- The first router hop displayed is the default gateway of the host from which the traceroute was executed. It is on a private network (10.10.8.1).
- The second hop is the router port on the external network (209.3.205.180).
- The remaining hops trace the route across the internet to the host.
- Connectivity to this host was reached in an acceptable time frame (130 milliseconds).

## nslookup

The `nslookup` (name server look up) command is an application that queries a DNS database for information about its DNS entries. This is useful if you suspect domain resolution or DNS configuration problems on a host. You can query any DNS server (if you know its name or IP address) but, by default, queries are run against the DNS server configured for the host requesting the lookup.

Typical use of the `nslookup` command for a Windows-based host is:

```
nslookup <ipaddress> <server>
```

or

```
nslookup <domainname> <server>
```

where

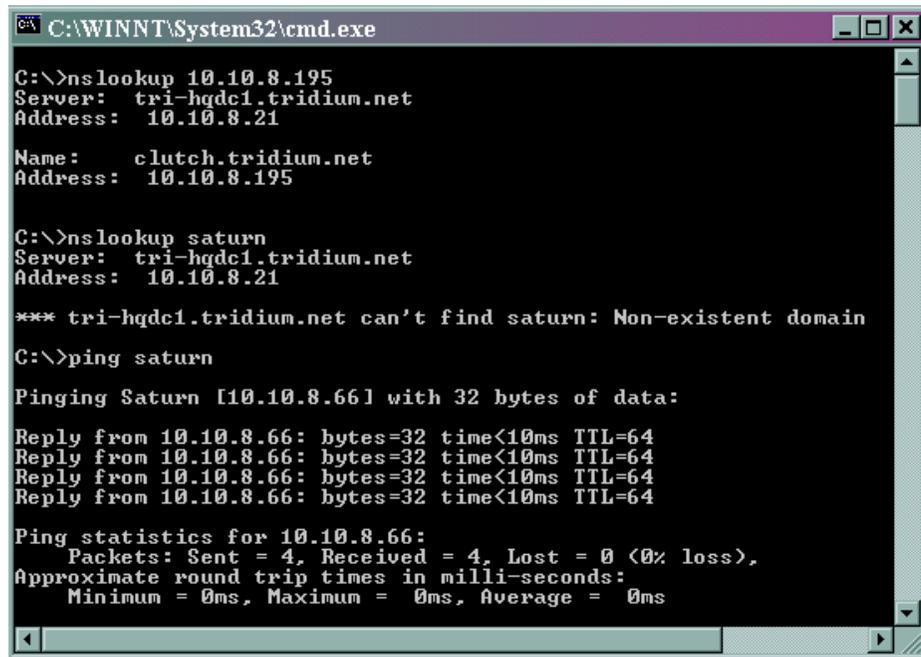
**<ipaddress>** is the IP address of a host you want information about.

**<domainname>** is the name of the host domain you want information about.

**<server>** is the name or IP address of a server other than the default. This parameter is optional.

Figure 2-14 shows two examples of an NSLookup to hosts on a local network.

Figure 2-14 NSLookup to internal hosts.



```
C:\WINNT\System32\cmd.exe

C:\>nslookup 10.10.8.195
Server: tri-hqdc1.tridium.net
Address: 10.10.8.21

Name: clutch.tridium.net
Address: 10.10.8.195

C:\>nslookup saturn
Server: tri-hqdc1.tridium.net
Address: 10.10.8.21

*** tri-hqdc1.tridium.net can't find saturn: Non-existent domain

C:\>ping saturn

Pinging Saturn [10.10.8.66] with 32 bytes of data:

Reply from 10.10.8.66: bytes=32 time<10ms TTL=64

Ping statistics for 10.10.8.66:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The following things are shown:

- In the first query, an IP address of 10.10.8.195 was used and the default name server replied with the FQDN of the host (clutch.tridium.net).
- The second query shows the response from the name server when a valid host is not listed on the server. In this case the name “saturn” was an name entry in the local hosts file, rather than in the DNS server.
- The ping example shows the availability of the host Saturn.

Figure 2-15 shows an example of an NSLookup about an external domain (bbc.co.uk).

Figure 2-15 NSLookup to an external domain.

```

C:\WINNT\System32\cmd.exe

C:\>nslookup bbc.co.uk ns.uu.net
(root) nameserver = D.ROOT-SERVERS.NET
(root) nameserver = A.ROOT-SERVERS.NET
(root) nameserver = H.ROOT-SERVERS.NET
(root) nameserver = C.ROOT-SERVERS.NET
(root) nameserver = G.ROOT-SERVERS.NET
(root) nameserver = F.ROOT-SERVERS.NET
(root) nameserver = B.ROOT-SERVERS.NET
(root) nameserver = J.ROOT-SERVERS.NET
(root) nameserver = K.ROOT-SERVERS.NET
(root) nameserver = L.ROOT-SERVERS.NET
(root) nameserver = M.ROOT-SERVERS.NET
(root) nameserver = I.ROOT-SERVERS.NET
(root) nameserver = E.ROOT-SERVERS.NET
D.ROOT-SERVERS.NET internet address = 128.8.10.90
A.ROOT-SERVERS.NET internet address = 198.41.0.4
H.ROOT-SERVERS.NET internet address = 128.63.2.53
C.ROOT-SERVERS.NET internet address = 192.33.4.12
G.ROOT-SERVERS.NET internet address = 192.112.36.4
F.ROOT-SERVERS.NET internet address = 192.5.5.241
B.ROOT-SERVERS.NET internet address = 128.9.0.107
J.ROOT-SERVERS.NET internet address = 198.41.0.10
K.ROOT-SERVERS.NET internet address = 193.0.14.129
L.ROOT-SERVERS.NET internet address = 198.32.64.12
M.ROOT-SERVERS.NET internet address = 202.12.27.33
I.ROOT-SERVERS.NET internet address = 192.36.148.17
E.ROOT-SERVERS.NET internet address = 192.203.230.10
*** Can't find server name for address 137.39.1.3: No information
Server: UnKnown
Address: 137.39.1.3

Name: bbc.co.uk
Served by:
- ns1.nic.uk
 195.66.240.130
 co.uk
- sec-nom.dns.uk.psi.net
 co.uk
- ns2.kpnqwest.net
 co.uk
- ns-nom.pipex.net
 158.43.128.74
 co.uk

```

The following things can be noted about this example:

- The query was run using another name server (ns.uu.net or 137.39.1.3).
- The query was run specifying information about a domain, rather than a host. Therefore, the name server replied with a list of the secondary-level name servers that know about the bbc.co.uk domain.

## netstat

The **netstat** utility is a TCP/IP utility available on most operating systems, including Windows. It is used to display protocol statistics and port usage of the local host.

In the Niagara environment, it can be used to troubleshoot port-related issues.

Typical syntax for the **netstat** command for a Windows-based host is:

```
netstat
```

or

```
netstat -n
```

where `-n` shows host information with IP addresses instead of names.

[Example 2-1](#) shows an example of `netstat` run at a command line of a Windows 2000 host called CLOBBER. It shows client connections open to many servers using different server-side ports. In this example, CLOBBER is a Web Supervisor and administration host and Saturn is a JACE-4/5.

Reference line information in the left column is used to facilitate the discussion which follows the example.

**Example 2-1 Netstat utility example.**

| Reference Line | Proto | Local Address | Foreign Address               | State       |
|----------------|-------|---------------|-------------------------------|-------------|
| 1              | TCP   | CLOBBER:4326  | intrepid.getresponse.com:http | CLOSE_WAIT  |
| 2              | TCP   | CLOBBER:4332  | Saturn:telnet                 | ESTABLISHED |
| 3              | TCP   | CLOBBER:4397  | Saturn:ftp                    | ESTABLISHED |
| 4              | TCP   | CLOBBER:4504  | popserv.mrf.mail.rcn.net:pop3 | TIME_WAIT   |
| 5              | TCP   | CLOBBER:4507  | Saturn:3011                   | TIME_WAIT   |
| 6              | TCP   | CLOBBER:4326  | Saturn:3011                   | ESTABLISHED |
| 7              | TCP   | CLOBBER:4484  | CLOBBER.tridium.net:8080      | ESTABLISHED |
| 8              | TCP   | CLOBBER:4488  | CLOBBER.tridium.net:8080      | ESTABLISHED |

The following things can be noted about this example:

- The protocol for each connection is TCP.
- The **Local Address** column lists the name of the local host (CLOBBER) followed by the client-side port number opened for the connection.
- The **Foreign Address** column lists the name of the host that CLOBBER is connected to and the port number opened on the server for the connection. Sometimes a name is listed rather than the port number. The name is the default function (as listed in [Table 1-10](#) on page 1-31) associated with the port. For example, in Line 3, CLOBBER is connected to Saturn via the file transfer protocol (FTP) on default port 21.
- As indicated in line 5, CLOBBER has opened a connection to Saturn using the Admin Tool on port 3011.
- CLOBBER (as a Web Supervisor) is running a Niagara station, but the default port for the station has been changed to 8080. Lines 7 and 8 indicate that CLOBBER has opened a browser or the JDE to the local station.

## Windows-specific

### ipconfig

The `ipconfig` (for IP configuration) command is a command-line utility available on Windows NT 4.0 and Windows 2000 hosts. It is used to report IP configuration information for the host. It shows information for all Ethernet adapters in the host.

**Tip**

---

For Windows 95/98 hosts, the `wipconfig` (Windows IP Configuration) program provides similar information. It is also a command-line utility.

---

Typical syntax for the IPConfig command for a Windows-based host is:

```
ipconfig
```

or

```
ipconfig /all
```

In addition, for Windows 2000 hosts, the following syntax can also be used to display the contents of the DNS cache on the local host, which can show the DNS entries this host has used recently.

```
ipconfig /displaydns
```

[Example 2-2](#) shows typical IPConfig information returned for a host:

**Example 2-2 IPConfig example.**

```

C:\>ipconfig /all

Windows 2000 IP Configuration

 Host Name : SATURN
 Primary DNS Suffix : tridium.net
 Node Type : Hybrid
 IP Routing Enabled. : Yes
 WINS Proxy Enabled. : No
 DNS Suffix Search List. : tridium.net

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix . : tridium.net
 Description : 3Com 3C920 Integrated
Fast Ethernet
Controller (3C905C-TX Compatible)

 Physical Address. : 00-B0-D0-F8-3A-C0
 DHCP Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IP Address. : 10.10.8.66
 Subnet Mask : 255.255.255.0
 Default Gateway : 10.10.8.1
 DHCP Server : 10.10.8.22
 DNS Servers : 10.10.8.21
 10.10.8.22
 Primary WINS Server : 10.10.8.22
 Lease Obtained. : Thursday, October 18,
2001 4:30:52 AM
 Lease Expires : Friday, October 19,
2001 4:30:52 AM

```

The following things can be noted about this example:

- The host is named Saturn and is a member of the tridium.net domain.
- The host is using DHCP to receive its IP settings. Lease information for the DHCP settings is also shown (for more information, see the [“Using the ipconfig Command”](#) section on page 3-31).
- This host also uses a WINS server for name resolution for legacy Windows hosts.

## Additional Information

For more information about the topics covered in this section, consult the sources listed in [Table 2-19](#).

**Note**

As with any web resource, addresses provided are subject to change. If a listed resource is unavailable, try a search for the article or concept using your favorite search engine.

**Table 2-19 Sources for more information about covered topics.**

| Concept                    | Source                                                                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Tool                 | "Getting Started with the Admin Tool" in the <i>Niagara Quick Start Guide</i>                                                                   |
| FTP                        | <a href="http://www.webteacher.org/winnet/ftp/ftpQ.html">http://www.webteacher.org/winnet/ftp/ftpQ.html</a>                                     |
| ipconfig, ping, traceroute | <a href="http://www.networkcomputing.com/netdesign/1123iprpart3.html">http://www.networkcomputing.com/netdesign/1123iprpart3.html</a>           |
| NetMeeting                 | <a href="http://www.microsoft.com/windows/netmeeting/features/default.asp">http://www.microsoft.com/windows/netmeeting/features/default.asp</a> |
| Telnet                     | <a href="http://www.webteacher.org/winnet/telnet/telnetQ.html">http://www.webteacher.org/winnet/telnet/telnetQ.html</a>                         |



## Connecting on a LAN

---

This chapter discusses connecting Niagara devices on the same enterprise LAN or WAN using the following main topics:

- [Niagara Considerations](#)
- [Connecting an Engineering PC](#)
- [Connecting a New JACE Controller](#)
- [Troubleshooting Connectivity to an Existing JACE Controller](#)
- [Using DHCP](#)

### Niagara Considerations

This section discusses typical system architectures and best practices when engineering Niagara environments. Before reading further, if you are not already familiar with networking and TCP/IP concepts, you may want to review [Chapter 1, “Understanding Networking and IP Addressing.”](#) If you are familiar with these concepts, you may want to review just the the “[Niagara Considerations](#)” section on page 1-32.

### System Architectures

[Figure 3-1](#) and [Figure 3-2](#) provide examples of typical Niagara job configurations (system architectures) for a single site (with a LAN) and multi-site (two LANs forming a WAN) environment.

#### Single site

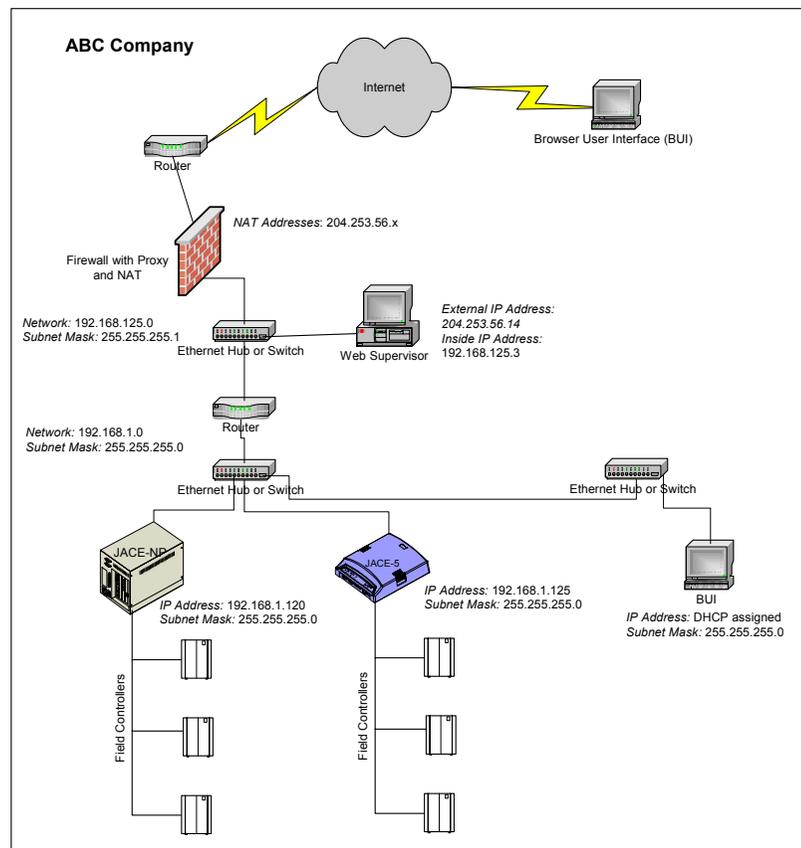
In the scenario presented in [Figure 3-1](#), a customer has a single site with a LAN, connecting to the Internet through a firewall. The firewall provides security, as well as network address translation (NAT), which provides company devices with public IP addresses so they can be accessed from the Internet.

The site has multiple JACE controllers controlling field devices. These JACEs have private IP addresses, and therefore cannot be accessed by the BUI user located across the Internet. However, they can be accessed by the BUI user located on the same LAN.

The Web Supervisor, on the other hand, has a public IP address assigned to it in the firewall. It can be reached by the BUI user located across the Internet (the external user) and also the internal BUI user. In this scenario, the Web Supervisor has been engineered to include GxPages showing real-time information originating from the JACEs. To accomplish this, the Niagara hosts use station-to-station (interstation) links. In addition, the Web Supervisor functions as a supervisory station, archiving other stations' data logs, alarms, etc. This data is available to either BUI user.

The network site administrator chose to place the Web Supervisor outside the enterprise LAN but just behind the firewall. This allows faster access by the external BUI user because the network traffic between the external host and the Web Supervisor does not come onto the customer's enterprise LAN (which may be congested).

**Figure 3-1 Typical single site (LAN) architecture.**

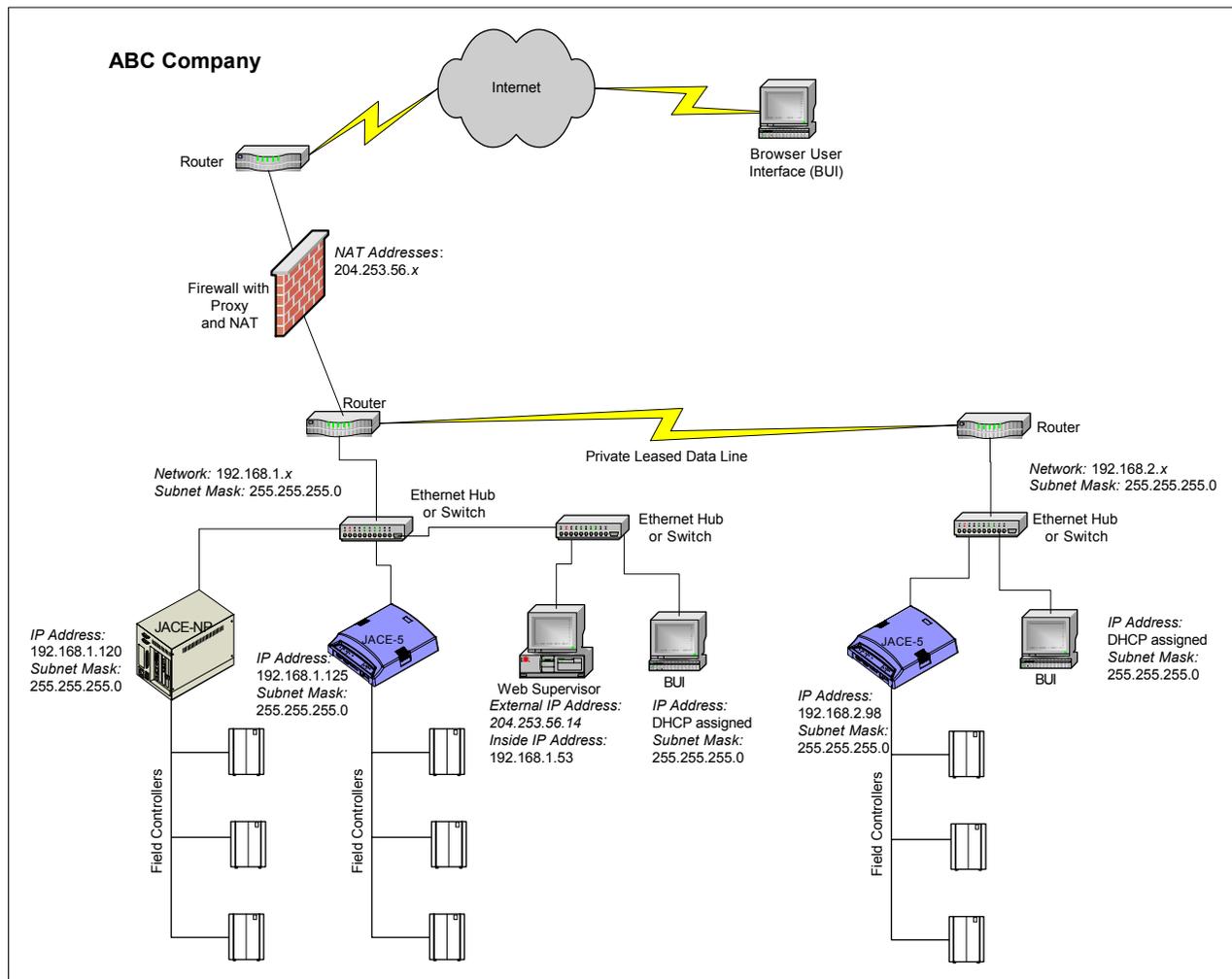


## Multiple sites

In the scenario presented in [Figure 3-2](#), ABC Company has added a JACE to a LAN at another site. The sites connect to each other using a private data line leased from a phone company, thereby creating an enterprise-wide WAN.

Interstation links are still used by all JACEs to update the GxPages on the Web Supervisor. However, the network site administrator decided to move the Web Supervisor onto the enterprise LAN at the primary site, since there was more data traffic generated internally than the occasional external BUI use. The internal IP address of the Web Supervisor changed to one in the IP range of the new network to which it is attached, but the external address (courtesy of NAT) did not change.

**Figure 3-2** Typical multi-site (WAN) architecture.



For additional information on engineering Niagara jobs, please see Chapter 1, “Engineering Strategies” of the *Niagara Web Solutions Guide*.

## Things to Note

You should note the following things about connecting Niagara devices to a LAN or WAN:

- Connection between Niagara hosts on a LAN/WAN will be faster and more reliable than connection via modem (either direct dial or through an ISP).
- Interstation links were designed to be used across connections that are always available. The design assumes that connections between linked hosts go up or down infrequently. **Therefore, interstation links should only be used on a LAN or WAN, and only on a LAN/WAN that provides reliable connection between hosts.**
- The key to success in many installations is early involvement by the IT department at the site. If you are going to connect devices to their LAN/WAN you need to check with them before implementing to learn about their policies so you can follow them.
- Access to hosts with private IP addresses can be made from hosts on the same LAN/WAN. Any host (Niagara or other) that needs to be accessed directly from the Internet must have a public IP address. External hosts can only access privately-addressed internal hosts through a virtual private network (VPN) (see [“Using a Virtual Private Network,”](#) page 6-4), or directly with dial-up (see [Chapter 4, “Connecting with Direct Dial”](#)).
- When connecting to Niagara hosts behind a firewall, certain ports need to be opened on the firewall for access by a BUI client or by an engineering station running the JDE or the Admin Tool. For more information on ports in the Niagara environment, see the [“Default Niagara Port Numbers”](#) section on page 6-7.
- There are limitations with using our equipment behind a true proxy server. For details, see [Chapter 6, “Using Security Technologies”](#).

## Using Niagara in a Microsoft Windows Server Environment

The following table provides a discussion of the impacts of Niagara hosts on a typical Microsoft Windows server environment using WINS, DNS, DHCP, or DDNS.

It is organized by the type of host, as most impact is dependent on the operating system running on the host.

Table 3-1 Niagara hosts in a Microsoft Windows Server Environment.

| Category          | Operating System                                                                                                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| JACE-NP           | <ul style="list-style-type: none"> <li>Embedded Windows NT 4.0</li> <li>Optional: Full version of Windows NT 4.0</li> </ul>                                                                                       | <p>Since the JACE-NP uses Windows NT 4.0 as its operating system, it operates in an Windows NT or Windows 2000 environment just like any other Windows NT 4.0 host. Specifically, it:</p> <ul style="list-style-type: none"> <li>can register with a WINS server for name resolution from other Windows hosts</li> <li>supports host name lookup on WINS and DNS servers</li> <li>can be a DHCP client</li> <li>cannot be a Windows DDNS or <a href="#">Active Directory</a> client<sup>1</sup></li> </ul> <p>By default, each JACE-NP is configured with the following settings:</p> <ul style="list-style-type: none"> <li>is a member of the workgroup named Workgroup</li> <li>has an pre-assigned IP address in the range 192.168.1.190-199 and a subnet mask of 255.255.255.0 and a default gateway of 192.168.1.1</li> <li>does not have any DNS or WINS servers defined</li> <li>is not a member of an Internet domain (for example tridium.com)</li> <li>DHCP client is installed but not enabled (see the <a href="#">“Using DHCP”</a> section on page 3-23)</li> <li>NetMeeting Remote Desktop Sharing is installed and enabled (Embedded Windows only)</li> <li>RAS is installed but not enabled</li> <li>SNMP client is installed and enabled (Embedded only)</li> <li>the Guest account is disabled</li> </ul> <p>In addition, the RCMD service has been configured and enabled on all JACE-NPs, but is used primarily with the full version of Windows NT 4.0 (See <a href="#">“Remote Command Utility”</a> on page 2-5).</p> <p>Many of these settings can be changed to accommodate the needs of a particular Windows environment.</p> <p><b>Note:</b> The Embedded JACE-NP cannot join a Windows Domain. It also has some restrictions on adding or configuring resources. For help with configuring an Embedded JACE-NP, contact Systems Engineering.</p> |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |
| JACE-4/5          | <table border="1"> <tr> <td>JACE-5</td> <td rowspan="2">WindRiver VxWorks</td> </tr> <tr> <td>JACE-4</td> </tr> </table>                                                                                          | JACE-5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | WindRiver VxWorks                                                                      | JACE-4        | <p>The JACE-4/5 is not a Windows host and therefore does not support WINS for name resolution of Windows hosts. However, it:</p> <ul style="list-style-type: none"> <li>supports host name lookup on a DNS server</li> <li>can be a DHCP client (see the <a href="#">“Using DHCP”</a> section on page 3-23)</li> <li>cannot be a Windows DDNS or Active Directory client.</li> </ul> |
| JACE-5            | WindRiver VxWorks                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |
| JACE-4            |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |
| Engineering PC    | <table border="1"> <tr> <td>Web Supervisor PC</td> <td rowspan="2"> <ul style="list-style-type: none"> <li>Windows NT 4.0</li> <li>Windows 2000</li> </ul> </td> </tr> <tr> <td>Technician PC</td> </tr> </table> | Web Supervisor PC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Windows NT 4.0</li> <li>Windows 2000</li> </ul> | Technician PC | <p>Since this host uses either Windows NT 4.0 or Windows 2000 as its operating system it operates in an Windows NT or Windows 2000 environment just like any other Windows NT 4.0 or Windows 2000 host. If this host is using Windows 2000, then it has the Windows NT 4.0 functionality plus the capability of being a DDNS and Active Directory client.</p>                        |
| Web Supervisor PC | <ul style="list-style-type: none"> <li>Windows NT 4.0</li> <li>Windows 2000</li> </ul>                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |
| Technician PC     |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                        |               |                                                                                                                                                                                                                                                                                                                                                                                      |

1. For more information about using our hosts with Internet DDNS, see the [“Niagara Considerations”](#) section on page 5-1.

## Windows NT and Windows 2000 Security

There are two levels of security in a Windows NT or Windows 2000 network. Each individual Windows NT or Windows 2000 host has local security. Login accounts that are added to local security have access only to resources on that host when they are logged on. Windows hosts have two initial local login accounts: Administrator and Guest.

The second level of Windows security is Windows Domain (in a Windows NT environment) or Active Directory (in a Windows 2000 environment) security. Accounts that are added to a Windows Domain or Active Directory (AD) can access both the local host and other hosts and resources in the Domain or Active Directory, when granted the appropriate permissions.

When a login account is added to either local or Domain/AD security, it can be assigned to a group. Groups are used to assign permissions for access to resources (like files or printers or e-mail) to like accounts. Both local and Domain/AD security contain several built-in groups that have special permissions. One of these groups is the Administrators group. An account in the Administrators group of either the local host or the Domain/AD has full permissions on the local host (if in the Administrators group of the local host) or the Domain/AD (if in that Administrator's group). The built-in Administrator account is a member of the Administrators group. The Guest account is in the Guests group, which has restricted permissions and can only access limited resources on the host.

Niagara was designed with support for local security **only** on all hosts. That makes our software portable to hosts running many different operating systems.

For Niagara hosts running Windows NT or Windows 2000, any Niagara host account that you create with the Users tab of the Admin tool is actually added to local Windows user security. This means you cannot use a Domain or AD user as an Niagara host administrator account. Further, any Niagara *administrator* account you add is actually added to the local Windows Administrators group, which means it has full permissions on the local host.

**Note**

---

By default, JACE-NPs ship with the two built-in accounts (Administrator and Guest). However, the Guest account is disabled (for security). In addition, another administrator account is present and enabled (on many hosts, this account is named **tridium**). This is the account you typically use to log into the host when using the Admin Tool.

---

## Connecting an Engineering PC

The following sections provide a brief overview of connecting an engineering PC to the LAN.

Typically, each engineering PC (be it a Web Supervisor or technician PC) will have a single NIC with a female 10/100-Mbit Ethernet connector. This provides the connection point of the PC to the Ethernet LAN.

### Windows NT 4.0

Use the following procedure to attach a Windows NT 4.0 engineering PC to a LAN. These instructions assume that the network card has been installed, Windows has been loaded, and TCP/IP networking has been installed.

**Procedure 3-1 Connecting a Windows NT 4.0 PC to an Ethernet LAN.**

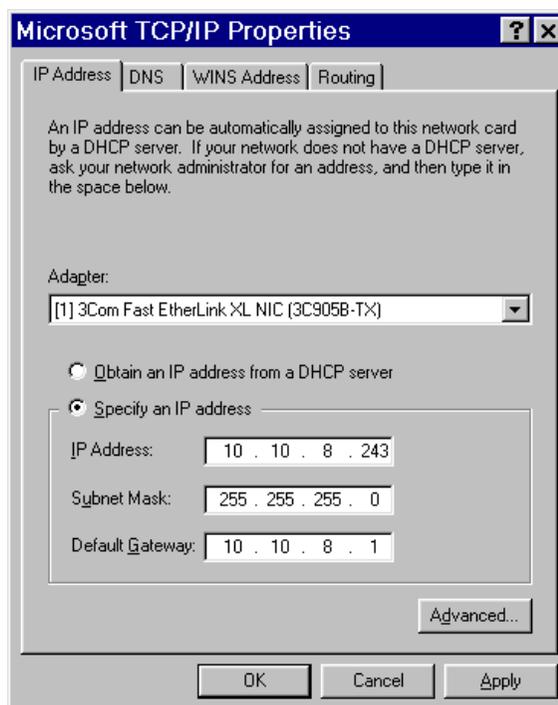
- Step 1** Attach one end of a standard Category-5 Ethernet unshielded twisted pair (UTP) patch cable to the RJ-45 connector on the PC.
- Step 2** Attach the other end of the patch cable to a network port or directly to an Ethernet hub.
- Step 3** Power up the PC.
- Step 4** Log into Windows NT with administrator access.



**Tip** If the JDE software has been loaded, you can use the administrator account for Niagara to log in. This account is an administrator on the PC.

- Step 5** On the desktop, right-click **Network Neighborhood** and choose **Properties**.
- Step 6** Click the **Protocols** tab.
- Step 7** Click **TCP/IP Protocol** and click the **Properties** button.
- Step 8** On the **IP Address** tab, fill out the network information (IP address, subnet mask, and gateway), or choose to get this information from a DHCP server (click **Obtain an IP address from a DHCP server**).

**Figure 3-3 Setting up TCP/IP on a Windows NT 4.0 host.**



- Step 9** On the remaining tabs, set DNS and WINS server information (if applicable).
- Step 10** When finished, click **OK**.

**Step 11** Reboot the PC.

---

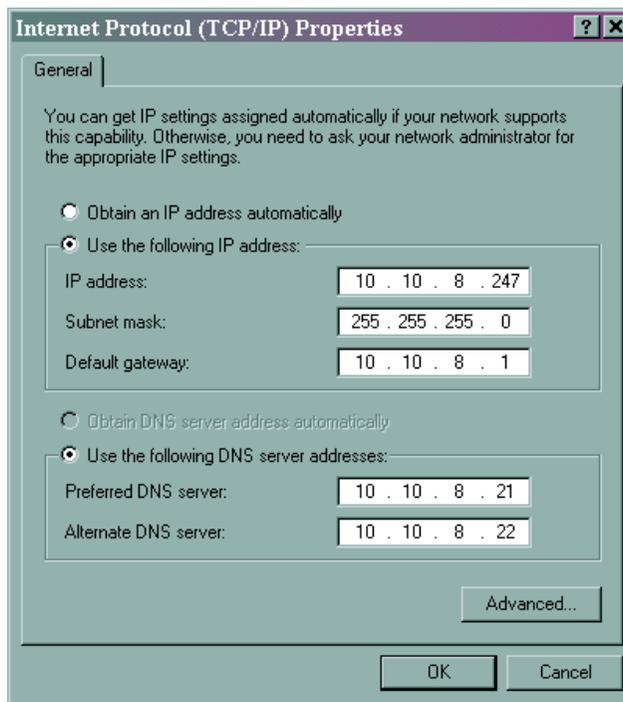
## Windows 2000

Use the following procedure to attach an Engineering PC to a LAN. This assumes that the network card has been installed, Windows 2000 has been loaded, and TCP/IP networking has been installed.

### **Procedure 3-2 Connecting a Windows 2000 PC to an Ethernet LAN.**

---

- Step 1** Attach one end of a standard Category-5 Ethernet unshielded twisted pair (UTP) patch cable to the RJ-45 connector on the PC.
- Step 2** Attach the other end of the patch cable to a network port or directly to an Ethernet hub.
- Step 3** Power up the PC.
- Step 4** Log in to Windows 2000 with administrator access.
-  **Tip** If the JDE software has been loaded, you can use the administrator account for Niagara to log in. This account is an administrator on the PC.
- 
- Step 5** On the desktop, right-click **My Network Places** and choose **Properties**.
- Step 6** Double-click **Local Area Connection**.
- Step 7** Click **Properties**.
- Step 8** Double-click **Internet Protocol (TCP/IP)**.
- Step 9** On the **General** tab, fill out the network information (IP address, subnet mask, and gateway), or choose to get this information from a DHCP server (click **Obtain an IP address automatically**).

**Figure 3-4** Setting up TCP/IP on a Windows 2000 host.

- Step 10** Click the **Advanced** button to set DNS and WINS server information (if applicable). Or, if you want to get this information from the DHCP server, click **Obtain DNS server address automatically**.
- Step 11** When finished, click **OK**.

The settings are changed. You do not need to reboot the PC.

## Connecting a New JACE Controller

A single, female 10/100-Mbit Ethernet connector is provided on each JACE, and provides the connection point of the JACE to the Ethernet LAN. This connection is capable of running at either 10 Mbps or 100 Mbps and will automatically adjust to the speed of the port on the hub into which it is plugged.

If for some reason you do not have access to a LAN you can also directly connect a PC to the JACE using an Ethernet [crossover cable](#). A crossover cable can be used to connect two computers together without a hub, or to connect two hubs together (if the hub does not have an uplink port).

## Determining the Default Network Information

JACE controllers are shipped with pre-assigned network settings. In most cases, this information will not be compatible with the network on which you are installing the equipment, and you will want to change it. But in order to change it, you first need to attach to the JACE using the pre-assigned network information.

In older units, the last digit of the IP address pre-assigned to the new JACE is the same as the last digit of the serial number of the unit. In units shipped more recently, the packing slip contains the IP address information.

Use the following table to determine default network configuration parameters for an older JACE.

**Table 3-2 Initial network parameters for JACE controllers.**

| JACE Series | Location of Serial Number on Unit      | IP Address Range               | Subnet Mask   |
|-------------|----------------------------------------|--------------------------------|---------------|
| JACE-NP     | On the back of the unit.               | 192.168.1.190 to 192.168.1.199 | 255.255.255.0 |
| JACE-5      | On the on the metal cover of the unit. | 192.168.1.140 to 192.168.1.149 | 255.255.255.0 |
| JACE-4      | On the on the metal cover of the unit. | 192.168.1.140 to 192.168.1.149 | 255.255.255.0 |

To change network settings on the new JACE, you must first connect it to an Ethernet LAN using a straight through Ethernet UTP patch cable or attach to it directly using a crossover cable. Then, use the Admin Tool from the Java Desktop Environment (JDE) to change the network settings.

### About Ethernet Straight Through and Crossover Cables

A 10/100BASE-T Ethernet port on a network interface card (NIC) uses 4 of the possible 8 pins in the RJ-45 female connector. Pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data. The port on a NIC is referred to as an MDI port.

An Ethernet port on a hub, however, is referred to as an MDI-X port because the pins transmitting and receiving data are crossed over. On an MDI-X port, pins 1 and 2 receive data and pins 3 and 6 transport data.

A standard Ethernet patch cable (used to connect a host and a hub) is wired straight through so that the transmit pins on a NIC connect to the receive pins on the hub, and vice versa.

Table 3-3 illustrates the pinouts of a host's Ethernet MDI port and a hub's Ethernet MDI-X ports and connection using a straight through cable. Note that the TX (transmit) function of the PC connects (via the straight through cable) to the RX (receive) function of the hub, and vice versa.

**Table 3-3 MDI to MDI-X connection.**

| NIC MDI port |             | Straight Through Cable Used to Connect Devices | Hub MDI-X port |          |
|--------------|-------------|------------------------------------------------|----------------|----------|
| Function     | Pin on Port |                                                | Pin on Port    | Function |
| TX+          | 1           | -----                                          | 1              | RX+      |
| TX-          | 2           | -----                                          | 2              | RX-      |
| RX+          | 3           | -----                                          | 3              | TX+      |
| RX-          | 6           | -----                                          | 6              | TX-      |



**Note** If you look at each end of a straight through cable, the ends would look identical because they are pinned out the same.

In order to connect two hosts together (with matching MDI ports), or to connect two hubs together (with matching MDI-X ports), you must use a crossover cable<sup>1</sup>. The cable takes care of connecting the transmit to the receive on the matching ports by crossing over the transmit and receive pairs within the cable.

Table 3-4 illustrates the pinouts of MDI ports on two hosts and the connection using a crossover cable. Note that the TX function of Host1 (on pins 1 and 2) connects via the crossover cable to the RX function of Host2 (on pins 3 and 6), and vice versa.

**Table 3-4 MDI and MDI-X pinouts.**

| Host1 MDI port |             | Crossover Cable Used to Connect Devices | Host2 MDI port |          |
|----------------|-------------|-----------------------------------------|----------------|----------|
| Function       | Pin on Port |                                         | Pin on Port    | Function |
| TX+            | 1           | -----                                   | 1              | TX+      |
| TX-            | 2           | -----                                   | 2              | TX-      |
| RX+            | 3           | -----                                   | 3              | RX+      |
| RX-            | 6           | -----                                   | 6              | RX-      |



**Note** The crossover cable has one end wired like a straight through cable, and one end wired differently.

1. Sometimes hubs have a special uplink port, used to connect hubs together. The uplink port actually is an MDI port rather than an MDI-X port. Use a straight through cable to connect the uplink port on one hub to a regular (MDI-X) hub port on another hub.

Ethernet straight through (also called standard) and crossover cables are widely available commercially. However, if you do not have a cable with you that you need you can use the information in [Table 3-5](#) to make up a cable. Both EIA/TIA 568A and 568B pinouts are given. The only real difference between 568A and 568B is that the White/Orange-Orange and White/Green-Green pairs are swapped.

To make a straight through cable, choose either the 568A or B pinout and make both ends to the same standard. To make a crossover cable, make one end following *each* standard.

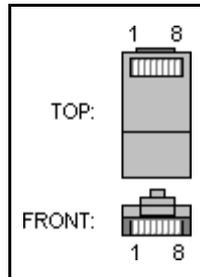
**Table 3-5 Ethernet cable pinouts.**

| Pin # | Signal                | EIA/TIA 568A           | EIA/TIA 568B           |
|-------|-----------------------|------------------------|------------------------|
| 1     | TX+                   | White/Green            | White/Orange           |
| 2     | TX-                   | Green or Green/White   | Orange or Orange/White |
| 3     | RX+                   | White/Orange           | White/Green            |
| 4     | Not used <sup>1</sup> | Blue or Blue/White     | Blue or Blue/White     |
| 5     | Not used              | White/Blue             | White/Blue             |
| 6     | RX-                   | Orange or Orange/White | Green or Green/White   |
| 7     | Not used              | White/Brown            | White/Brown            |
| 8     | Not used              | Brown or Brown/White   | Brown or Brown/White   |

1. Even though the wires connected to these pins are not used, you should connect them anyway.

The following figure provides a pin reference for an RJ-45 (male) connector.

**Figure 3-5 RJ-45 male pin reference.**



## Connecting to the LAN and Assigning the IP Address

Use the following procedure to attach the JACE to a LAN, assign its working IP address, and verify connectivity.

### Procedure 3-3 Connecting a JACE controller to an Ethernet LAN.

- 
- Step 1** Attach one end of a standard Category-5 Ethernet unshielded twisted pair (UTP) patch cable to the RJ-45 connector on the JACE.
- Step 2** Attach the other end of the patch cable to a network port or directly to an Ethernet hub.



---

**Note** The maximum end-to-end distance from the JACE to the hub is 328 feet (100m).

---

**Step 3** Power up the JACE controller.



---

**Note** The JACE-4/5 controller identifies itself to the Ethernet LAN during power up. If the controller is powered up prior to making this connection, the unit will not be accessible on the network. With the Ethernet connector plugged in, disconnect the power connector, allow the controller to completely power down (no status LEDs are blinking), and reconnect the power connector.

---

**Step 4** Assign the IP address of your engineering station in the range of 192.168.1.1 to 192.168.1.254. However, do not duplicate the IP address already assigned the JACE, or assigned to another host on the LAN.

**Step 5** Start the **Admin Tool**.

- a. Click the **Start** button on the taskbar and expand the **Programs** menu to view the Niagara folder.
- b. Click the **Admin Tool** icon to launch the **Admin Tool**.

**Step 6** In the **Admin Tool** view, click **File** on the menu, and click **Open**.

A connection dialog box is displayed.

**Step 7** Type the pre-assigned IP address of the JACE and click **OK**.

**Step 8** Log onto the JACE controller with the initial user name and password, which is listed on the packing slip. Click **OK**.



---

**Note** For many units, the initial user name is **tridium** and the default password is **niagara**.

---

The JACE controller (IP address) appears in the Admin Tool view as an open host.

**Step 9** Click the **Network Settings** tab.

**Step 10** Assign the JACE a unique IP address and other network settings to be used for communications.

For more information on these settings, see the “[Networking using IP](#)” section on page 1-16.



---

**Caution** Be very careful when typing in this information. If you make a mistake you could make the host unreachable (see “[Troubleshooting Connectivity to an Existing JACE Controller](#),” page 3-14). Be sure to document the network settings that you do use.

---

Once you have made changes to one or more network settings, you must reboot the host for those changes to be implemented. The Admin Tool provides a reboot function on the Host menu.

- Step 11** From the menu, select **Admin Tool > Host > Reboot** to implement your changes.
- Step 12** Change the network settings on your PC to be in the same range as the new IP address for the JACE.
- Step 13** Using the ping command, ping the IP address of the JACE.  
For more information on the ping command, see the “ping” section on page 2-20.

## Crossover Cable Connection

Use the following procedure to attach an engineering PC directly to the JACE and verify connectivity:

### Procedure 3-4 Connecting to a JACE using a crossover cable.

- Step 1** Connect one end of an Ethernet crossover cable to the Ethernet port on the JACE.
- Step 2** Connect the other end of the crossover cable to the Ethernet port on your engineering PC.
- Step 3** Follow [Step 3—Step 13](#) of [Procedure 3-3](#).

## Troubleshooting Connectivity to an Existing JACE Controller

In a typical environment, once you set up a JACE on the network you will always be able to reach it across the LAN using its documented IP address or name. However, you might walk into a customer environment for which you do not have documentation. Or, the JACE may have become unreachable at the documented settings.

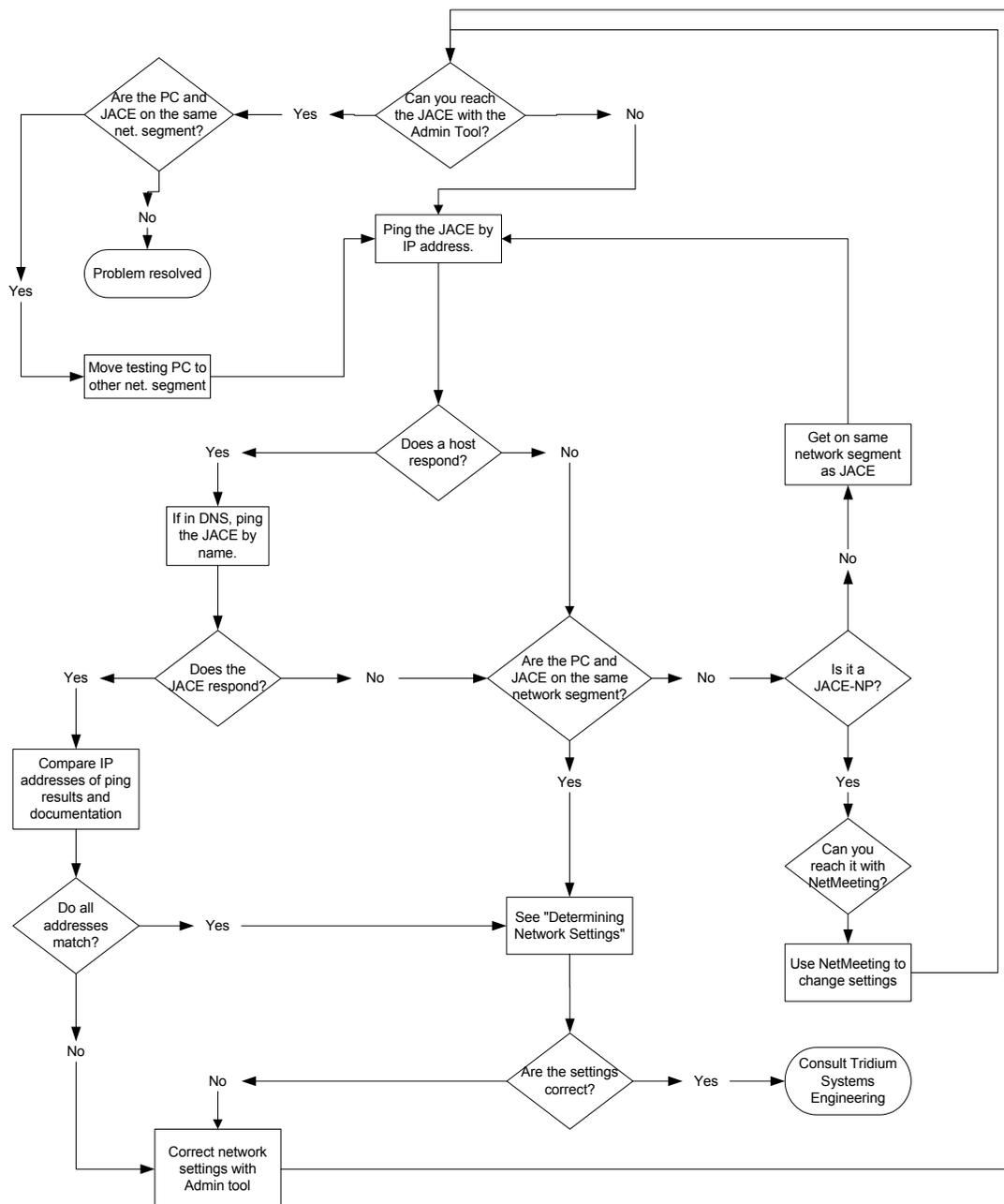
In addition, when typing in the network settings for a host, it is quite common to make a typing error in the IP address, subnet mask, or default gateway. A mistake in any one of these settings could make your host unreachable. Consider the following scenarios:

- **Mistake in IP address**—If you make a mistake when typing the IP address, the host will be reachable at the incorrect address, but not at the correct address. You would need to know how to look up the IP address it was configured with to be able to connect to it to correct the address (see “[Determining Network Settings](#)”).

- Mistake in subnet mask or default gateway**—If you make a mistake when typing either of these pieces of information, the host will be reachable on the same network segment of the LAN, but will be unreachable by machines on other segments (including from a WAN or from the Internet). In addition, the host will be unable to initiate communications with hosts on other segments. You would need to attach to the same network segment as the JACE and fix the mistake using the Admin Tool.

Figure 3-6 provides a decision flowchart to help you troubleshoot these type of connectivity problems with JACEs.

Figure 3-6 Troubleshooting decision matrix.



## Determining Network Settings

If you are unsure of the network settings on a JACE controller, first attempt to connect to the JACE at the default IP address (see the “[Determining the Default Network Information](#)” section on page 3-10). The previous installer may have left the controller at those settings for convenience.

If you changed the IP address of the JACE using the Admin Tool, but are unsure what you changed it to, you can look in the `ipchanges.txt` file to figure it out.

### About the `ipchanges.txt` file

The `ipchanges.txt` file is created or updated in the `<x>:\niagara\<release>\nre\user` directory of your engineering workstation whenever you change the IP address of a host using the Admin Tool (release 2.2 or later). This file lists:

- the time and date of the change
- the user who was logged in when the change was made
- the old and new IP addresses
- the name of the host that was changed

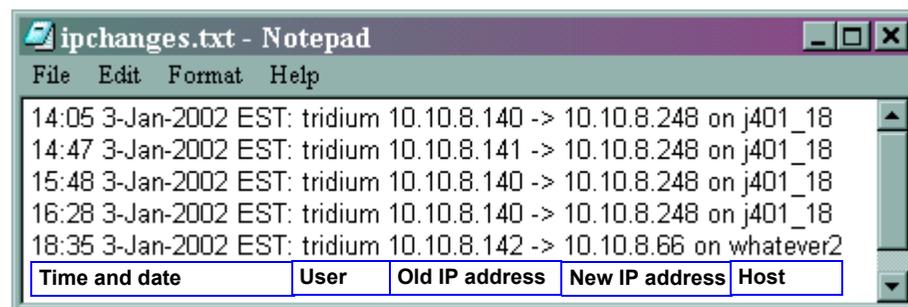
Figure 3-7 shows an example of two hosts whose IP addresses were changed.



#### Notes

- An `ipchanges.txt` file can exist for each release you have installed on your PC. If you cannot find the file in the current release directory, check previous release directories. You may have changed the IP address using a previous release.
- The `ipchanges.txt` file only records IP address changes you make using the Admin Tool. It will not record a change made with another method (such as Windows networking tools).

Figure 3-7 IPchanges.txt file.



If you cannot connect to the JACE using either of these two methods, then use the model-specific information that follows to help you find this information.

## JACE-NP

There are two methods you can use to track down misplaced network settings for a JACE-NP. One is fairly easy to implement, but it assumes you know some information about the JACE. The other is more complex, but assumes you know little information about the JACE.

### Method 1 (Easy)

Each JACE-NP ships from the factory with one of the following default names:

- **NPenumber**—for embedded NT models shipped after December 2000
- **NPnumber**—for full NT models and earlier versions of the embedded model
- **NPmnumber**—for models with a modem (these also have full NT)

In addition, when shipped, the NP is a member of a Windows workgroup named **Workgroup**. If these default settings have not been changed (or if only one of them has been changed) you may be able to browse the Windows Network to determine the name of the JACE. Then you can use the TCP/IP ping utility to help you find the IP address, and the Admin Tool tool to determine the subnet mask and default gateway.



**Note** This procedure only works if you know the network portion of the JACE's IP address (for example, 192.168.1.x).

#### Procedure 3-5 Determining an IP address for an unknown JACE-NP.

**Step 1** On your engineering station, connect to the same Ethernet hub as the JACE-NP. Alternately, connect to the JACE with a crossover cable.



**Note** Microsoft workgroup information is spread via broadcast and many routers are configured to prevent this information from being forwarded to another network segment. Therefore, in order to browse the workgroup the JACE is in, you must be on the same network segment.

**Step 2** Using one of the methods described in [“Connecting an Engineering PC”](#), change the IP address settings on your engineering station to match those of the customer's LAN, or those of the JACE (see the first note in this section).

Your PC is now in the same IP address range of the JACE you are trying to reach.

**Step 3** Using one of the following methods, open a window to browse the network:

- **Windows NT 4.0**—Double-click **Network Neighborhood** on the desktop.
- **Windows 2000**—Double-click **My Network Places** on the desktop.

**Step 4** Double-click **Entire Network**.

**Step 5** Double-click **Microsoft Windows Network**.

**Step 6** Double-click **Workgroup**.

You see the list of machines belonging to the Workgroup workgroup. JACE-NPs have names beginning with NP.

- Step 7** If you do not see the name of the JACE you are looking for (or any JACE), click the **Back** button of the Workgroup window and search in other listed workgroups and domains for your JACE-NP. Otherwise, continue with the next step.
- Step 8** Open a command prompt (see [Procedure 2-12](#)).
- Step 9** Ping the JACE by name (see the “ping” section on page 2-20).  
The ping command returns the IP address of the JACE you pinged.
- Step 10** Connect to the JACE using the Admin Tool and change the incorrect network settings as described in “[Connecting a New JACE Controller](#),” page 3-9.
- 

## Method 2 (Complex)

If you cannot find the JACE by browsing the Windows network, you can use a TCP/IP packet sniffer to capture IP packets. A packet sniffer analyzes network traffic and provides a list of devices attempting to talk to one another, regardless of the network address they are using. A sniffer can either be a hardware device or software that runs on your PC.

Once you capture some packets, you can examine the capture and look for IP addresses outside of the customer’s network range. Once you have a list of rogue IP addresses you can attempt to connect to the hosts with either the Admin Tool or NetMeeting.

Some things to note about using a packet sniffer:

- Packet sniffers can be used both for troubleshooting (as in this example) and for malicious purposes. The customer’s IT department may have a strong objection to you using one on their network, therefore, it is advisable to check with them before using a sniffer on their network.
- The information presented by the sniffer is complex and may not be readily understandable by a networking novice. Many IT departments regularly use packet sniffers, therefore they may be able to get you the information that you need.

If the IT department cannot help you, however, you can use the following procedure as a guide to getting the information you want with a packet sniffer.

### Procedure 3-6 Finding an IP address using a packet sniffer.

---

- Step 1** Connect the TCP/IP packet sniffer to the same network as the JACE. The sniffer can either be a hardware device, or your PC running packet capture software.
- Step 2** Capture packets on the network for 5 minutes or longer.
- Step 3** Examine the capture. Typically you will see a list of source IP addresses (the host address that the packet was coming from) and destination IP addresses (what address the packet was heading to).
- Step 4** If possible in your sniffer, sort the list by the source IP address.

- Step 5** Look for any IP addresses that fall outside the customer's normal network address range, and that are unfamiliar to you (i.e., not another host that you already know about).
- Since the JACE-NP is a Windows device, it sends out regular broadcast messages to any master browser. These messages are sent to the broadcast address of the network range the NP is in. For example, if the source address of the NP is 199.81.168.128 (with a Class C subnet mask of 255.255.255.0), then the broadcast address is 199.81.168.255. For an NP addressed as 172.20.15.1/255.255.0.0 (Class B), the broadcast address is 172.20.255.255. For more information on broadcast addresses, see the “[Special IP Addresses](#)” section on page 1-22.
- Step 6** Change your engineering PC's IP address to the same network range of a likely IP address.
- Step 7** Try to connect to the IP addresses with the Admin Tool or NetMeeting.
- 

## JACE-4/5

Since the JACE-4/5 does not run Windows as its OS, Windows networking will not provide the name of a JACE-4/5. If a JACE-4/5 has been added to a DNS server (and you know the name of it) you can still use the ping command to determine the IP address. However, if you do not know the name or it is not in DNS, you can still determine the IP address and subnet mask by connecting to the VxWorks target shell and reading them, because they are displayed during the boot sequence.



### Caution

Be **very** careful when using the target shell on a JACE-4/5. You must log on to the JACE with administrative privileges, which means you can change many settings. Changes you make could have unexpected consequences, including making the JACE inoperable.

---

### Procedure 3-7 Determining an IP address of a JACE-4/5.

---

- Step 1** Using Hyperterminal on your engineering station, connect to the VxWorks command shell following [Step 1](#) to [Step 12](#) of [Procedure 2-5](#).
- Step 2** When you see text appear in the Hyperterminal window, do not break out of the boot sequence as described in [Step 13](#) of that procedure. Instead, allow the controller to finish booting.
- The controller displays startup messages similar what you see in the Standard Output Window of the Admin Tool.
- Step 3** When the controller stops displaying new messages, press **ENTER** to reach the command prompt.
- You see a prompt similar to the following:
- >
- Step 4** Using the scroll bars on the Hyperterminal window, scroll up until the section that begins with the line **Press any key to stop auto-boot...** (see [Figure 3-8](#)).

**Figure 3-8** IP address read from a Hyperterminal boot sequence.

```

JACE-45 - Hyper Terminal
File Edit View Call Transfer Help

Press any key to stop auto-boot...
0
auto-booting...

boot device : tffs=0,0
unit number : 0
processor number : 0
file name : /tffs/sys/j401rel
inet on ethernet (e) : 10.10.8.248:FFFFFF00
user (u) : anonymous
ftp password (pw) : user
flags (f) : 0x8
target name (tn) : j401_18
other (o) : fei

Attaching to TFFS... done.
Loading /tffs/sys/j401rel...2360244
Starting at 0x100000...

Attached TCP/IP interface to fei unit 0
Attaching interface lo0...done
Loading symbol table from /tffs/sys/j401rel.

Connected 0:25:49 Auto detect 9600 8-N-1 SCROLL CAPS NUM

```

The IP address of the JACE is listed on the line that begins **inet on ethernet (e) :**. The IP address is listed (in dotted decimal), followed by a colon, and then the subnet mask (in hexadecimal). For information on deciphering the subnet mask, see [“Converting the Subnet Mask from Hexadecimal”](#).

- Step 5** After making note of the IP address, disconnect from the application and reboot the JACE as described in [Procedure 2-6](#).
- Step 6** Connect to the JACE using the Admin Tool and change the faulty network settings as described in Chapter 4 of the *Niagara Quick Start Guide*.

## Converting the Subnet Mask from Hexadecimal

When the IP address displays during the VxWorks boot process, it is in dotted decimal format (i.e. 10.10.8.248). However, the subnet mask is in plain hexadecimal format, with no delimiter between each octet (FFFFFF00 rather than FF.FF.FF.00). Use the following procedure to convert the subnet into dotted decimal format.

### Procedure 3-8 Converting hexadecimal subnet mask to dotted decimal form.

- Step 1** On your engineering PC, open the Windows calculator.
- Step 2** From the menu, select **View > Scientific**
- Step 3** Click the **Hex** (hexadecimal) radio button.

- Step 4** Type the first two characters of the hexadecimal number (this is the first octet).  
For example, if the number displayed is FFFFFFFC0, you would type FF.
- Step 5** Click the **Dec** (decimal) radio button.
- Step 6** Read and record the value displayed.  
In the example, FF (hex) converts to 255 (decimal). This is the first octet, or 255.
- Step 7** Continue converting (if necessary) and recording each pair of characters, inserting a period between each octet.  
The example converts to 255.255.255.192
- 

## Other Access Methods

If you cannot reach the JACE after troubleshooting using the methods described previously, the next sections describe some other techniques you can use for accessing JACEs.

### JACE-NP

As a last resort, if you are running an NP with the full version of Windows NT 4.0, you can connect a keyboard, mouse, and monitor to the unit, reboot and log in. This is not an option for a JACE-NP running embedded NT because it does not recognize these devices.

If you cannot reach a JACE-NP with the Admin Tool, NetMeeting, or by logging in, consult Systems Engineering.

### JACE-4/5

If for some reason a JACE-4/5 is not accessible over the LAN, you can connect to a JACE-4/5 with Hyperterminal and a null modem connection and change the IP address and subnet mask. This may make it available again.

Use the following procedure to change these network settings using Hyperterminal.



**Caution** Be **very** careful when using the target shell on a JACE-4/5. You must log on to the JACE with administrative privileges, which means you can change many settings. Changes you make could have unexpected consequences, including making the JACE inoperable.

---

#### Procedure 3-9 Changing network settings using Hyperterminal.

---

- Step 1** Using Hyperterminal on your engineering station, connect to the VxWorks command shell as described in [Procedure 2-5](#).
- Step 2** At the [VxWorks Boot:] prompt, type:  
[VxWorks Boot:] **c**  
This puts the JACE in system change mode.



**Tip** If you do not break the boot sequence in time and the JACE fully starts up, you can press **ENTER** to get to the command prompt (->), then type **bootChange** to enter system change mode.

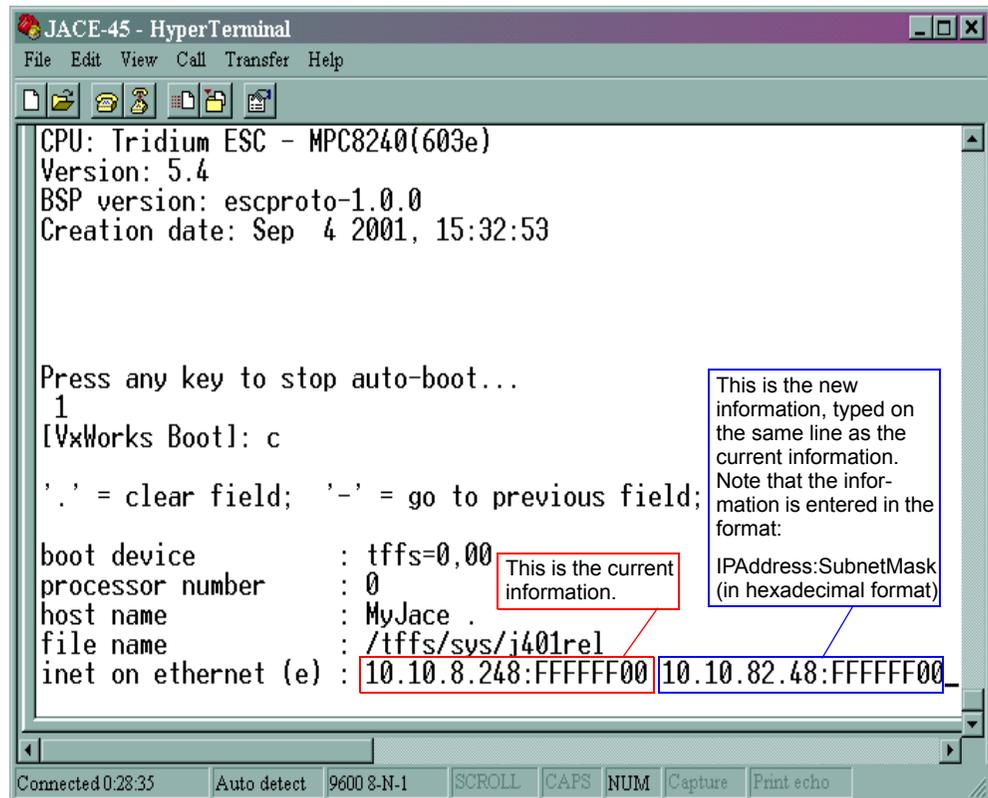
**Step 3** Press **ENTER**.

**Step 4** Press **ENTER** to scroll through each field of the system settings until you reach the fifth field, **inet on ethernet (e)**.

You see the current IP address and subnet mask, separated by a colon. (See [Figure 3-8](#) and “[Converting the Subnet Mask from Hexadecimal](#)”).

**Step 5** On the same line as the address information, type the new address information in the same format as it appears ([Figure 3-9](#)).

**Figure 3-9** Changing the IP address and subnet mask.



**Step 6** To accept your changes, press **ENTER**. If you do not want to update the information, backspace to erase any changes you made and press **CTRL-D** to return to the VxWorks Boot prompt. Skip to [Step 8](#) in this procedure.

**Step 7** If you want to review or edit the information you changed in [Step 5](#), type a dash (-) on the **inet on backplane (b)** field, and press **ENTER** to return to the **inet on ethernet (e)** field. Otherwise, skip to [Step 8](#).

**Step 8** When finished, disconnect from the application and reboot the JACE as described in [Procedure 2-6](#).

**Step 9** Verify connectivity to the JACE by connecting with the Admin Tool.

---

If you cannot reach a JACE-4/5 with the Admin Tool after making these changes, consult Systems Engineering.

## Using DHCP

Dynamic Host Configuration Protocol (DHCP) is an Internet standard used to aid in configuring IP hosts. For more information about DHCP, see the “[Static and Dynamic IP Addressing](#)” section on page 1-25.

## Niagara Considerations

DHCP is supported by the operating systems used by all Niagara hosts. However, the following notes apply:

- Static IP addresses provide the most reliable connectivity between Niagara hosts. Problems can develop, for example, if one station is assigned a new IP by the DHCP server and it has links to other stations. Those links stop working until those stations are restarted. The DHCP server should be configured to allocate the same IP address to the Niagara host whenever it requests one. Note that this address is not really a static IP address, but rather is a dynamic one reserved by the DHCP server for the particular host.
- For the DHCP administrator to set up the reserved IP address, you will need to provide the MAC address of the Niagara host to the DHCP administrator (see “[Determining the MAC Address](#)”).
- You can set up DHCP on a JACE-4/5 with the Admin Tool but you must use Windows networking tools to set up DHCP on any Niagara host running the Windows OS.
- Windows 2000 DHCP servers can be configured to update DNS servers on behalf of devices that do not support dynamic update. JACEs do not support Dynamic DNS updates as defined in RFC 2136. JACE-4/5s do support Dynamic DNS (through a 3<sup>rd</sup> party) when using a dial-up ISP account to connect to the Internet (see the “[Configuring DDNS on the JACE-4/5](#)” section on page 5-22).

### Determining the MAC Address

Use the following procedure to determine the MAC address of a Niagara host.

**Procedure 3-10 Determining the MAC address of a Niagara host.**

---

- Step 1** Attach your engineering station to the same network segment as the Niagara host.
- Step 2** Open a Windows command prompt.
- Step 3** Ping the Niagara host at its current IP address (see “[ping,](#)” page 2-20).

**Step 4** At the command prompt, type the following command:

```
arp -a
```

You see information about the pinged host (and other hosts with which you have communicated). [Figure 3-10](#) shows an example of the information produced from the arp command after a host has been pinged.

**Figure 3-10** Ping and ARP commands executed to host 10.10.8.140.

```

C:\WINNT\System32\cmd.exe
Reply from 10.10.8.140: bytes=32 time<10ms TTL=64
Reply from 10.10.8.140: bytes=32 time<10ms TTL=64

Ping statistics for 10.10.8.140:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Interface: 10.10.8.247 on Interface 0x1000003
Internet Address Physical Address Type
10.10.8.21 00-60-cf-20-a4-69 dynamic
10.10.8.22 00-60-cf-20-bc-be dynamic
10.10.8.23 00-d0-b7-b9-07-3a dynamic
10.10.8.29 00-b0-d0-aa-d8-38 dynamic
10.10.8.140 00-01-f0-ff-ff-12 dynamic

```

**Step 5** In the **Internet Address** column, find the IP address of the host you pinged. The MAC address for the host is the 12-digit hexadecimal number listed in the adjacent **Physical Address** column. For [Figure 3-10](#), the MAC address of the pinged host (10.10.8.140) is 00-01-f0-ff-ff-12.

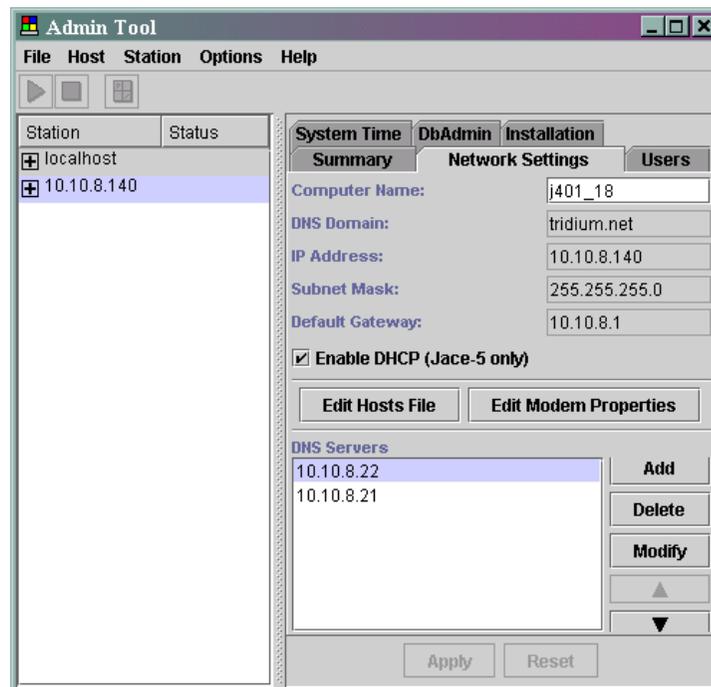
## Using DHCP on a JACE-4/5

The following things should be noted about using DHCP on a JACE-4/5:

- The JACE-4/5 DHCP client has been tested against the Windows NT and Windows 2000 Server DHCP implementations only. However, there are no known incompatibilities with other DHCP servers.
- The DHCP server **must** be configured to provide the JACE with the following information:
  - IP address
  - subnet mask
  - DNS server list
  - DNS domain name
  - default gateway
- The JACE **cannot** receive its host name from the DHCP server.

- When DHCP is enabled on a JACE-4/5, you cannot change the settings for IP address, subnet mask, default gateway, or DNS domain name using the Admin Tool because these settings are unavailable (see Figure 3-11). You can change the list of DNS servers, but upon reboot, the list will be refreshed with information from the DHCP server. To change any of these parameters, disable DHCP and manually set all of them.

Figure 3-11 Network Settings tab of Admin Tool on a JACE-4/5 host using DHCP.



The DHCP server is providing DNS domain, IP address, subnet mask, default gateway and DNS servers to this JACE-4/5.

## Configuring the JACE-4/5

Use the following steps to enable DHCP on the JACE-4/5.

### Procedure 3-11 Enabling DHCP on a JACE-4/5.

- Step 1 Open the Admin Tool.
- Step 2 Connect to the JACE using the factory assigned IP address.
- Step 3 On the **Network Settings** tab, click the **Enable DHCP** check box and click **Apply**.
- Step 4 Reboot the host.
  - a. From the Admin Tool menu, choose **Host > Reboot**.
  - b. Click **Yes** on the confirmation dialog box.
  - c. If prompted to back up the station, enter the name and password for the station administrator and click **OK**.

The JACE reboots.

- Step 5** Reconnect with the Admin Tool using the IP address assigned by the DHCP server. The DHCP administrator can tell you this address, or you can figure it out (see [“Determining Network Settings”](#)).
- Step 6** Verify that the network configuration parameters (DNS servers, etc.) have been properly assigned.
- 

## Trouble-shooting DHCP Problems on the JACE-4/5

This section discusses common DHCP problem scenarios on the JACE-4/5 and approaches to resolving them.

### Lease Renewal Failure

Per the DHCP specification, the JACE will periodically renew its lease, even when using a reserved address. The DHCP server defines the length of the renewal period. If the renewal request ever fails (for example, if the DHCP server is offline, or the Ethernet cable is disconnected when the renewal request occurs) and the lease expires, then, per the DHCP specification, the JACE disables its network interface. The DHCP specification was written that way to prevent a host from using an IP address for which it no longer has a valid lease.

When a JACE has failed to renew its lease, it cannot be accessed using the Ethernet connection and the heartbeat LED blinks rapidly. To fix this problem, correct the problem that caused the renewal to fail, and reboot the JACE.

### DHCP Reservation not Working

If the DHCP administrator has set up the reserved address, but the JACE fails to pick it up on the initial boot after you enabled DHCP, then you may have given the DHCP administrator the wrong MAC address. Verify the MAC address of the JACE using the previous procedure, or with the `ifshow` command (see [“Using Target Shell Commands”](#)).

However, if the JACE receives the reserved IP address, but upon renewal of its DHCP lease gets assigned another IP address, then the fault may lie with the DHCP reservation. If the DHCP server is Windows-based, the reservation must be made on both the primary DHCP server and any backup DHCP servers that handle the same DHCP scope. A DHCP scope is a range of IP addresses that the server can assign. If the scope can be assigned from multiple servers, then each server must also have reservations listed for the scope. To determine which DHCP server handled the last DHCP request for the JACE, see the `dhcpcParamsShow` command.

## Using Target Shell Commands

You may find it necessary to troubleshoot the DHCP settings of a JACE-4/5. Several commands are available from the VxWorks target shell for this purpose. To execute the commands listed in this section, connect to the Target Shell of the JACE as described in “[Hyperterminal](#),” page 2-7, then type the command (without spaces) at the prompt.

**ifShow**—Displays the MAC address of the JACE-4/5.

### Example 3-1 The ifShow command.

```
-> ifShow
fei (unit number 0):
 Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
 Type: ETHERNET_CSMACD
 Internet address: 10.10.8.248
 Broadcast address: 10.255.255.255
 Netmask 0xff000000 Subnetmask 0xff000000
 Ethernet address is 00:01:f0:ff:ff:12
 Metric is 0
<snip>
```

The MAC address is the 12-digit hexadecimal number in the highlighted line.

**dhcpcServerShow(pDhcpcBootCookie)**—Displays the IP address of the DHCP server being used.

### Example 3-2 The dhcpcServerShow(pDhcpcBootCookie) command.

```
-> dhcpcServerShow(pDhcpcBootCookie)
DHCP server: 10.10.8.21
value = 0 = 0x0
```

The DHCP server is listed in the highlighted line.

**dhcpcParamsShow(pDhcpcBootCookie)**—Displays the configuration data assigned to the JACE by the DHCP server.

**Example 3-3 The dhcpcServerShow(pDhcpcBootCookie) command.**

```
-> dhcpcParamsShow(pDhcpcBootCookie)
DHCP server name:
Boot file name:
DNS domain name: tridium.net
Router discovery enabled.
RFC 894 Ethernet encapsulation enabled.
Maximum datagram size: 576
Default IP Time-to-live: 64
Interface MTU: 576
ARP cache timeout: 60
Default TCP Time-to-live: 64
TCP keepalive interval: 7200
Client lease origin: 4
Client lease duration: 604800
Client renewal (T1) time value: 302400
Client rebinding (T2) time value: 529200
DHCP server: 10.10.8.21
Assigned IP address: 10.10.8.142
Client subnet mask: 255.255.255.0
Client router solicitation address: 255.255.255.255
Client IP routers:
 10.10.8.1
Client DNS name servers:
 10.10.8.22
 10.10.8.21
value = 0 = 0x0
```

All highlighted items are assigned to the JACE by the DHCP server. Highlighted items are discussed below:

- **DNS domain name**—the DNS domain for this host. This is also listed in the DNS Domain field in the Admin Tool.
- **Client lease duration**—the duration of the DHCP lease, in seconds. To convert the number to days, divide the number by 60, then by 60, then by 24.
- **Client renewal (T1) time value**—the amount of time left before the JACE attempts to renew the lease. The time is listed in seconds. If the lease is not renewable at this time, then the JACE will reset this timer and continue attempting renewal until the lease expires (see next parameter).

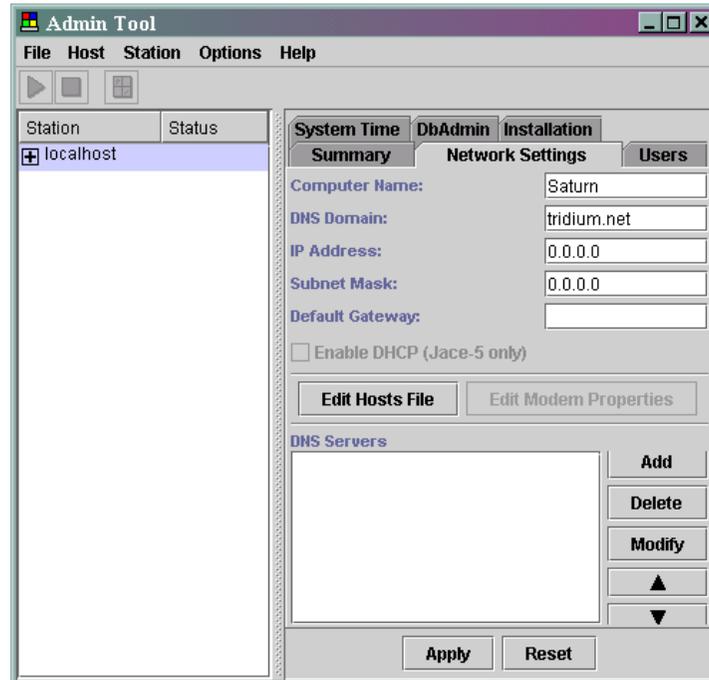
- **Client rebinding (T2) time value**—the amount of time left on the DHCP lease. The time is listed in seconds. If this time expires before the JACE can renew its lease, the Ethernet interface is disabled.
- **DHCP server**—the DHCP server that handled the last DHCP request.
- **Assigned IP address**—the IP address that the DHCP server assigned to the JACE.
- **Client subnet mask**—the subnet mask that the DHCP server assigned to the JACE.
- **Client IP routers**—the default gateway that the DHCP server assigned to the JACE. This is also listed in the Default Gateway field in the Admin Tool.
- **Client DNS name servers**—the DNS servers that the DHCP server assigned to the JACE. This is also listed in the DNS Servers field in the Admin Tool.

## Using DHCP on a Windows-based Niagara Host

The following things should be noted about using DHCP on a Windows-based Niagara host:

- You cannot use the Admin Tool to set up DHCP on a Windows-based Niagara host. You must use Windows networking tools to set up DHCP on any Niagara host running the Windows OS.
- Some settings provided by the DHCP server will show as 0 or blank on the Network Settings tab of the Admin Tool (see [Figure 3-12](#)). To review the settings that the DHCP server is providing to the Windows client, use the `ipconfig` tool (see [“Troubleshooting DHCP Problems on the JACE-NP,”](#) page 3-30).
- The DHCP server can be configured to provide any or all of the following information:
  - host name
  - IP address
  - subnet mask
  - default gateway
  - DNS server list
  - DNS domain name

**Figure 3-12** Network Settings tab of Admin Tool on a Windows-based Niagara host using DHCP.



The DHCP server is providing DNS domain, IP address, subnet mask, default gateway and DNS servers to this Windows-based Niagara host.

## Configuring an Engineering PC

See [“Connecting an Engineering PC”](#) for instructions on how to set up DHCP on any an Engineering PC.

## Configuring a JACE-NP

Use the following steps to set up DHCP on a JACE-NP.

### Procedure 3-12 Configuring DHCP on a JACE-NP.

- 
- Step 1** Connect to the JACE-NP desktop, as described in the [“NetMeeting”](#) section on page 2-2.
- Step 2** Follow the steps in [Procedure 3-2](#) to configure DHCP for a Windows NT 4.0 host.
- 

## Trouble-shooting DHCP Problems on the JACE-NP

This section discusses common DHCP problem scenarios on the JACE-NP and approaches to resolving them.

## Lease Renewal Failure

Per the DHCP specification, a Windows host will periodically renew its lease, even when using a reserved address. The DHCP server defines the length of the renewal period. If the renewal request ever fails (for example, if the DHCP server is offline, or the Ethernet cable is disconnected when the renewal request occurs) and the lease expires, then one of the following things occurs:

- **Windows NT 4.0 host**—disables its network interface. This follows the DHCP specification, and it was written that way to prevent a host from using an IP address for which it no longer has a valid lease.

When a host has failed to renew its lease, it cannot be accessed using the Ethernet connection. To fix this problem, correct the problem that caused the renewal to fail, and reboot the host.

- **Windows 2000 host**—the computer assigns itself an IP address in the private Class B range of 169.254.0.0 with a subnet mask of 255.255.0.0. No gateway or DNS server is assigned. This is a new feature of Windows 2000 called automatic IP addressing.

To fix this problem, correct the problem that caused the renewal to fail. When the DHCP server becomes able to service requests, the host will update its address information.

## DHCP Reservation not Working

If the DHCP administrator has set up the reserved address, but the JACE fails to pick it up on the initial boot after you enabled DHCP, then you may have given the DHCP administrator the wrong MAC address. Verify the MAC address of the host using [“Determining the MAC address of a Niagara host,”](#) page 3-23 or with the `ipconfig` command (see the next section [“Using the ipconfig Command”](#)).

However, if the JACE receives the reserved IP address, but upon renewal of its DHCP lease gets assigned another IP address, then the fault may lie with the DHCP reservation. In the DHCP server is Windows-based, the reservation must be made on both the primary DHCP server and any backup DHCP servers that handle the same DHCP scope. A DHCP scope is a range of IP addresses that the server can assign. If the scope can be assigned from multiple servers, then each server must also have reservations listed for the scope. To determine which DHCP server handled the last DHCP request for the JACE, see the `ipconfig` command.

## Using the ipconfig Command

The primary troubleshooting utility used with DHCP on a Windows-based host is `ipconfig` (see the [“ipconfig”](#) section on page 2-27). In [Example 3-4](#), information concerning the DHCP setup of a Windows 2000 host is highlighted (similar information is available for a Windows NT 4.0 host). A discussion of each highlighted item follows the example.

**Example 3-4 DHCP settings shown with the ipconfig command for Windows 2000 host.**

```

C:\>ipconfig /all

Windows 2000 IP Configuration

 Host Name : WEBSUP1
 Primary DNS Suffix : tridium.net
 Node Type : Hybrid
 IP Routing Enabled. : Yes
 WINS Proxy Enabled. : No
 DNS Suffix Search List. : tridium.net

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix . : tridium.net
 Description : 3Com 3C920 Integrated
Fast Ethernet
Controller (3C905C-TX Compatible)

 Physical Address. : 00-B0-D0-07-D0-A9
 DHCP Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IP Address. : 10.10.8.182
 Subnet Mask : 255.255.255.0
 Default Gateway : 10.10.8.1
 DHCP Server : 10.10.8.22
 DNS Servers : 10.10.8.21
 10.10.8.22
 Primary WINS Server : 10.10.8.22
 Lease Obtained. : Tuesday, January 08,
2002 9:52:57 AM
 Lease Expires : Tuesday, January 15,
2002 9:52:57 AM

```

- **Host Name**—the name of this host. This could be set manually or can be set from the DHCP reservation.
- **Connection-specific DNS Suffix**—the DNS domain as provided by the DHCP server.
- **Physical Address**—the MAC address of this host.
- **DHCP Enabled**—whether DHCP is enabled for this host.
- **IP Address**—the IP address of this host. This can be set manually or set by the DHCP server.
- **Subnet Mask**—the subnet mask of this host. This can be set manually or set by the DHCP server.

- **Default Gateway**—the default gateway of this host. This can be set manually or set by the DHCP server.
- **DHCP Server**—the IP address of the DHCP server that handled this host's last renewal request.
- **DNS Servers**—a list of DNS servers used for DNS lookups by this host. This information can be set manually (if automatic DNS not enabled) or provided by the DHCP server.
- **Primary WINS Server**—a list of WINS servers used for WINS lookups by this host. This information can be set manually (if automatic DNS not enabled) or provided by the DHCP server.
- **Lease Obtained**—the time and date the DHCP lease was obtained from the DHCP server.
- **Lease Expires**—the time and date when the DHCP lease expires.

You can also use the `ipconfig` command to force a renewal of the DHCP lease. This can be useful when you want to force the host to refresh its settings from the DHCP server (for instance, if a DNS server IP address changes). To do this, type the following at a command line:

```
ipconfig /renew
```



## Connecting with Direct Dial

---

A Niagara host can connect to other Niagara devices by dialing them directly. This can be the only connection between hosts, or be a supplementary connection (a secondary connection to a host already on a LAN).

This chapter covers how to set up these devices for direct access. It includes the following topics:

- [Niagara Considerations](#)
- [Configuring Direct Dial on the JACE-4/5](#)
- [Configuring Direct Dial on the JACE-NP](#)
- [Configuring Direct Dial on an Engineering PC](#)
- [Using Direct Dial](#)

This section does not cover connecting a Niagara host to an Internet service provider. You can find that information in [Chapter 5, “Connecting to an ISP.”](#)

### Niagara Considerations

This section discusses typical system architectures and best practices when connecting Niagara devices with direct dial. It includes the following topics:

- [System Architectures](#)
- [About Dialing between Niagara Hosts](#)
- [Design Considerations](#)

Before reading further, if you are not already familiar with connecting Niagara devices on a LAN, you may want to review [Chapter 3, “Connecting on a LAN.”](#)

## System Architectures

Figure 4-1 and Figure 4-2 provide examples of typical Niagara job configurations (system architectures) for connecting Niagara hosts through direct dial.

In the scenario presented in Figure 4-1, ABC Company has added two additional JACE-4/5s to remote sites (see the “System Architectures” section on page 3-1 for a description of the first two sites). These remote sites do not have a LAN and do not have a connection to site 1 with a private leased line like site 2 does. Instead, direct dial has been set up on both the Web Supervisor (at site 1) and the JACEs (in sites 3 and 4). This allows the JACEs to dial the Web Supervisor whenever they need to send archives or alarms. This setup also allows the Web Supervisor to dial the JACEs to acknowledge alarms, to maintain the devices using maintenance tools such as Admin Tool, JDE, or web browser, or to pick up archives, if polled archiving is set up.

Figure 4-1 Multiple JACE-4/5s connecting with direct dial to a Web Supervisor for HMI and alarm and archive purposes.

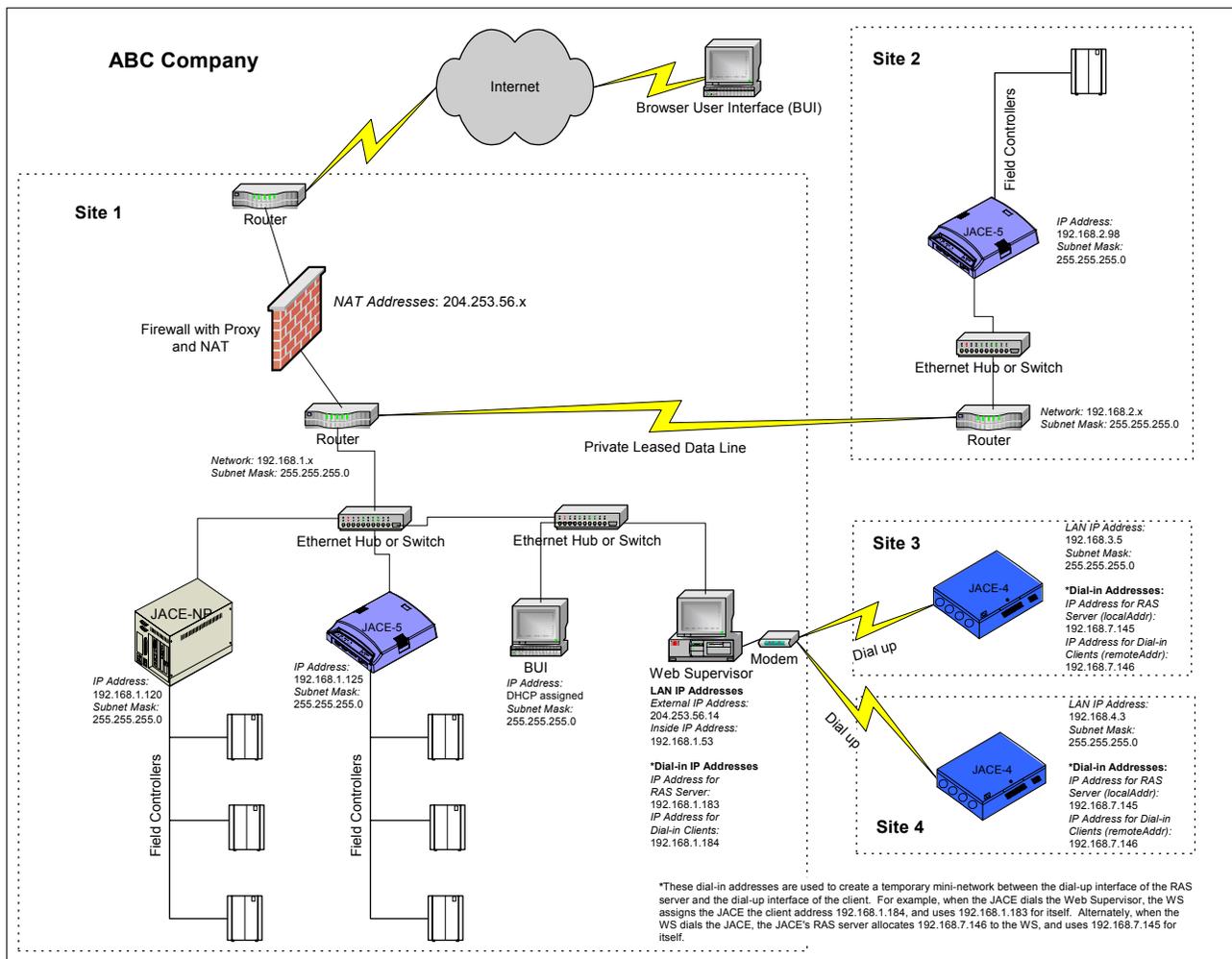
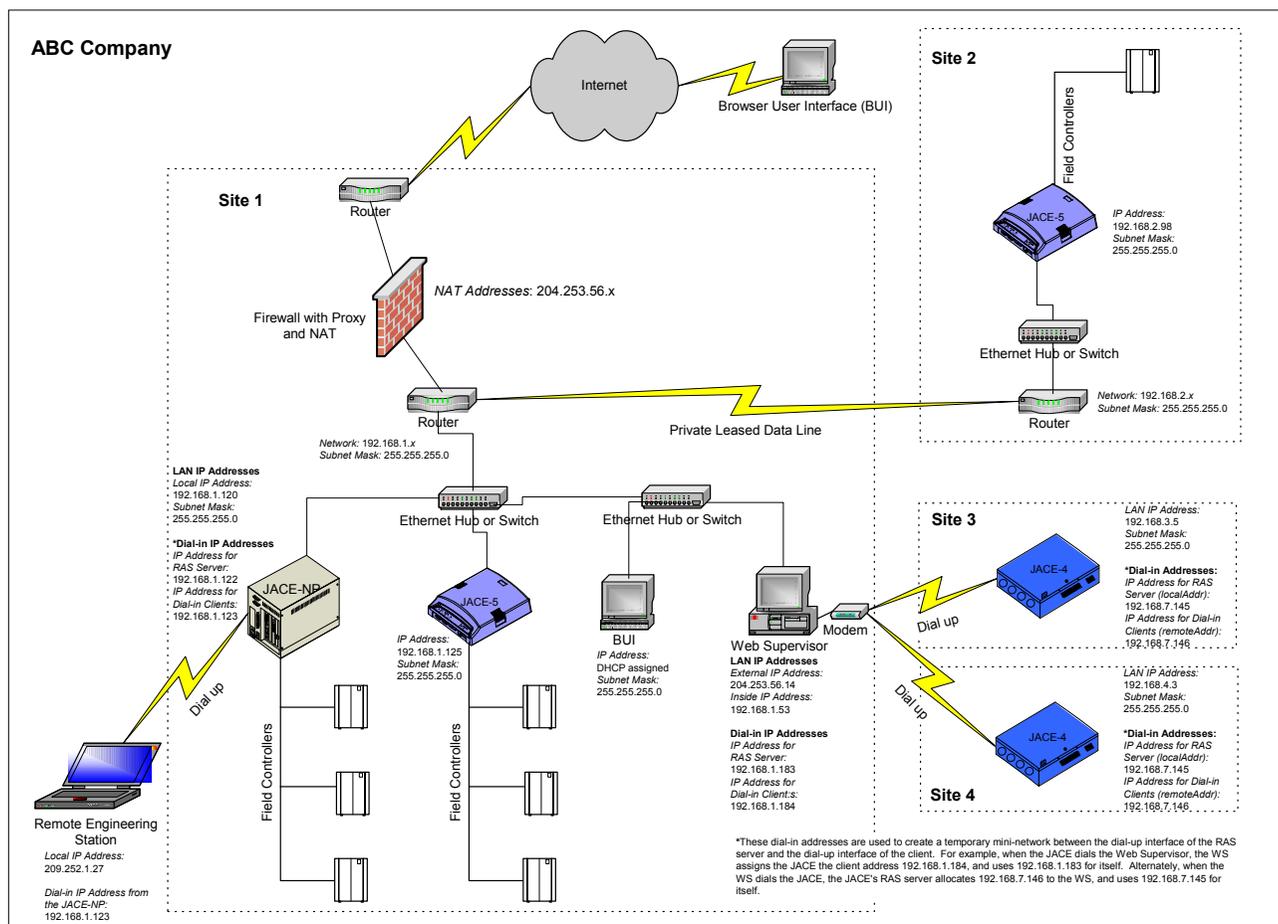


Figure 4-2 shows another typical implementation of dial-up. A systems integrator (SI) has configured a JACE-NP at Company ABC for dial-in. Choosing the JACE-NP for dial-in allows the SI to maintain not only the JACE-NP, but the other Niagara hosts on the LAN/WAN (sites 1 and 2). This is because Windows Remote Access Service (RAS) on the JACE-NP has been configured to allow any host that dials into it full access to its network. The SI chose not to dial into the Web Supervisor (where dial-in was already configured) because the connection is frequently busy with traffic from the remote JACE-4/5s.

There is one limitation with dialing into the NP, however. The JACEs in sites 3 and 4 are not maintainable through this connection by the remote SI. However, the remote engineering station can dial directly into the JACE-4/5s to maintain them.

Figure 4-2 Support by remote administration.



## About Dialing between Niagara Hosts

Any Niagara host can both dial another host and also be dialed into. As illustrated above, the JACE-4/5s dial out to deliver alarms and archives. They also are dialed up by the Web Supervisor and remote engineering station for maintenance. The Web Supervisor is also dialed into and dials out. On the other hand, the remote engineering

station will always dial-up the JACE-NP (or JACE-4/5s), but it will never be dialed into. This is not a function of the machine, or its dial configuration, but rather is a function of the information that it sends or receives.

In the examples above, two JACE-4/5s are shown dialing into one Web Supervisor, however, only one of them is connected at any one time. When one JACE is connected to the dial-in host (in this case, the WS), and the second JACE attempts to dial in, the second JACE continues to retry the dial-out until it is successful. After several failed connection attempts, the “wait between dials” time will increase to a maximum of 2 minutes. As soon as a connection is made, the wait time for the JACE is reset back to just a few seconds.

## User- versus Application-initiated Connections

You can also think of the connections between direct-dial hosts as user-initiated or application-initiated. Application-initiated connections are Niagara station-to-station connections. Examples include:

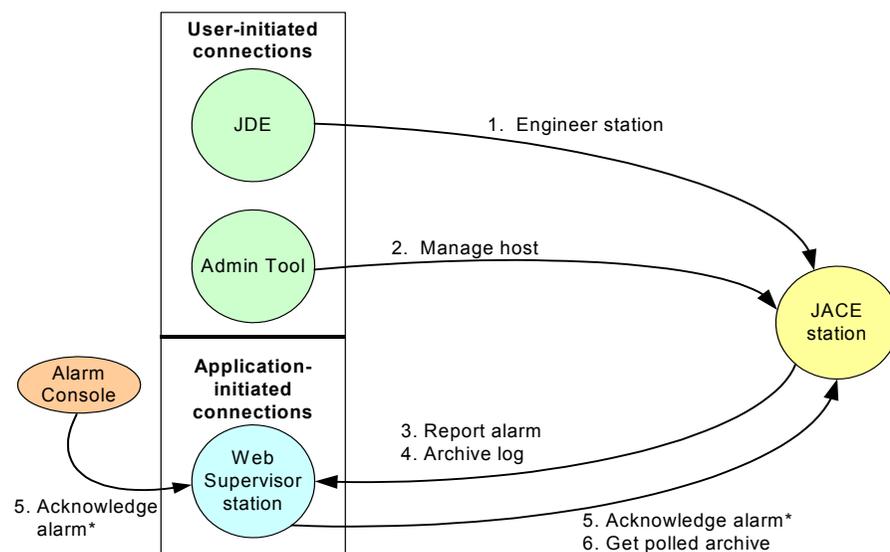
- a station on a JACE dialing a Web Supervisor station to deliver log archives or alarms.
- a station on a Web Supervisor dialing a JACE station to deliver an alarm acknowledgement.

Examples of user-initiated connections include:

- a user on the Web Supervisor or remote engineering host using the JDE to engineer a job on a remote JACE.
- a user on an engineering host using the Admin Tool to manage a host (start, stop, change settings, etc.).

These concepts are illustrated in [Figure 4-3](#).

**Figure 4-3 User- and application-initiated connections between direct-dial stations.**



\* The operator acknowledges the alarm with the Alarm Console, then the Web Supervisor station sends the acknowledgement to the JACE station, making it an application-initiated connection.

Only a single connection between a host and a remote Niagara software component can exist at one time. For example, if a JACE-4/5 has dialed a Web Supervisor to deliver alarms, you cannot use JDE on the same connection to access a JACE. Conversely, if the Web Supervisor runs the Admin Tool and dials into a JACE, the JACE will not be able to deliver alarms to the Web Supervisor on the same connection. These restrictions exist even if the GUI component (Admin Tool or JDE) is running on the same PC as the Web Supervisor station. Therefore, if you are on a user-initiated connection from the Web Supervisor to the JACE, alarms will queue in the JACE station for delivery by a subsequent application-initiated connection. In addition, any alarm acknowledgements processed on the Web Supervisor while user-connected will also queue in the WS station until the station has a chance to make an application-initiated connection. Polled archive requests will also queue until the user on the Web Supervisor releases the manual connection.

In all cases, user-initiated connections have priority over application-initiated connections. After each connection initiated by an application there is a period of time (5 minutes) when application-initiated re-connects are prohibited. There is also a maximum connect time (10 minutes) for application-initiated connections. After this time expires, the connection will be terminated automatically. This prevents a station rapidly generating alarms from monopolizing the modem and locking out dial-in user access.



---

**Note** You cannot modify these parameters.

---

## Design Considerations

You should note the following things about connecting Niagara hosts with direct dial:

- Connection between hosts using direct dial will be slower than connection on a LAN/WAN.
- If the hosts will use long-distance to dial each other, it may be cheaper to connect the hosts to local ISPs and connect through the Internet (see [“Connecting to an ISP,”](#) page 5-1). Some factors to consider are:
  - does each host have access to a local dial-in number to the ISP? Otherwise, long distance charges for any non-local host will be a factor.
  - will the JACEs be sending much data (archives and alarms)? If not, connecting long distance briefly, even several times a day may be cheaper than the ISP’s monthly fee.
- If you need frequent access to a remote host, consider connecting the host to an ISP. An ISP-connected host is virtually always available. In addition, an ISP-connected host does not have the same user- versus application-initiated restriction. With an ISP-connected host, user and application data can travel simultaneously.
- Support for ISDN, which provides faster dial-up connection, is available for any Windows-based Niagara host, but is not available for JACE-4/5s.

- The pass through management feature (which allows you to manage Niagara hosts on the same LAN once you are dialed into a Niagara host) is not available on the JACE-4/5s. It is a function of Windows RAS.
- Many IT departments prohibit setting up dial-up on hosts attached to their network. This is considered by many departments to be a network security violation. Therefore, it is advisable to check with them before implementing dial-up between hosts.

### Support for Interstation Links

Hosts that use dial-up to connect to other hosts do so only on demand. For instance, a JACE in site 3 or 4 only initiates a connection to the Web Supervisor when it has an alarm or archive to deliver. Conversely, the Web Supervisor will initiate a connection only when it is used to maintain the hosts or answer an alarm. Therefore, connections between hosts will connect and disconnect frequently.

**Since interstation links were designed to be used across connections that are always available, you cannot use them with direct dial.** When designing a station you will be unable to make an interstation link to any host configured for dial-up in the station address book.

Because interstation links are not available, if you require BUI access to remote hosts you must license WebUI services on each remote JACE.

### Connecting Multiple JACEs to One Web Supervisor

When you design a job with multiple JACEs dialing a single modem on a Web Supervisor or JACE-NP you must keep in mind that the connection is shared. We recommend that you:

- carefully plan your archiving strategy. For instance you could,
  - use daily archiving, but stagger archive times for each JACE so they are not attempting to send archives at the same time.
  - limit the size of the logs so they do not time out when reaching the maximum connect time for application-initiated connections.
  - use trigger objects to send archives more frequently than daily so they are not as large as a full day's file.
- limit the number of JACEs connecting to a WS by how “busy” you expect them to be. You can connect more lightly-loaded JACEs (ones that produce fewer alarms and smaller or less frequent archive files) but fewer heavily-loaded JACEs (ones that potentially alarm more and create larger or frequent archive files).
- review your connection strategy after it has been running for a period of time. If you find that the JACEs are not delivering information in a timely manner, either add more modems to the Web Supervisor, or add additional Web Supervisors.

If you find that you have too much traffic from the JACEs on a single connection you can:

- set up multiple modems on a single Web Supervisor to handle additional incoming and outgoing calls. However, this requires the server version of the Windows operating system (either Windows NT 4.0 Server or Windows 2000 Server).
- add additional Web Supervisors or JACE-NPs.

## Configuring Direct Dial on the JACE-4/5

This section guides you through installing and configuring modems and configuring the Niagara software for direct dial on the JACE-4/5. It has the following topics:

- [Installing and Configuring Modems](#)
- [Configuring the Software](#)

## Installing and Configuring Modems

Because they both use the VXWorks OS, the procedures for installing and configuring modems on the JACE-4 and JACE-5 are similar. However, there are some dissimilarities:

- The JACE-5 only supports external modems attached to an RS-232 port. The JACE-4 supports either an on-board (internal) modem or an external one.
- Configuring the JACE-4 requires an extra step because, by default, the on-board modem is not enabled. See the “[Enabling the JACE-4 Modem \(Internal or External\)](#)” section on page 4-10.

The following sections will help you configure modems on either the JACE-4 or JACE-5:

- [About Pre-configured Modems](#)
- [Enabling the JACE-4 Modem \(Internal or External\)](#)
- [Attaching an External Modem](#)

### About Pre-configured Modems

By default, the following modems are configured on the JACE-4 and JACE-5:

- **JACE-4**—Cermetek 2056 ET (its internal modem)
- **JACE-5**—U.S. Robotics Sportster

In addition, the the “[About the ras.properties File](#)” section on page 4-12 provides information about using a Zoom External V.90 Dualmode Faxmodem (Model 2949L).

While it is possible to connect modems of other types or brands, doing so may cause you some configuration difficulty. Modem configuration on the JACE-4/5 requires a modem initialization string which sets parameters that we require for proper operation. We provide the initialization string for the above referenced modems, or

ones that implement the [AT command set](#) in the same way (see the next section “[About the AT Command Set](#)”). You would need to provide the correct initialization string for any non-listed modem.

For example, this is the initialization string we use for the US Robotics Sportster:

```
AT&F1E0&A1X4
```

A breakout of the parameters set in this string is listed in [Table 4-1](#).

**Table 4-1 US Robotics Sportster initialization string.**

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AT            | The prefix used to tell the modem that one or more commands follow.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| &F1           | Use the hardware control flow template. This template sets the modem to hardware flow control, a fixed serial port rate, the highest level result codes, and the most complete result-code set.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| E0            | Sets the command mode echo to off. The modem does not display keyboard commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| &A1           | These settings enable ARQ error codes, which allows the modem to detect flawed data and retransmit it. It also returns connection rates to the modem as follows:<br><br>10/CONNECT 2400—Connection at reported rate. Other valid options include 18/CONNECT 4800, 13/9600, 20/7200, 21/12000, 25/14400, 43/16800, 85/19200, 91/21600, 99/24000, 103/26400, 107/28800.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| X4            | Sets the result codes that are returned from the modem to our hardware as follows: <ul style="list-style-type: none"> <li>• 0/OK—Command has been executed.</li> <li>• 1/CONNECT—Connection established with another modem</li> <li>• 2/RING—Incoming ring detected.</li> <li>• 3/NO CARRIER—Carrier may not be detected or carrier has been dropped due to disconnect.</li> <li>• 4/ERROR—Command is invalid.</li> <li>• 5/CONNECT 1200—Connection established with another modem at 1200 bps.</li> <li>• 6/NO DIAL TONE—Dial tone not detected during the normal 2 seconds, set in Register S6.</li> <li>• 7/BUSY—Busy signal detected; modem hangs up.</li> <li>• 8/NO ANSWER—After waiting 5 seconds for an answer, the modem hangs up; returned instead of NO CARRIER when the @ dialing option is used.</li> </ul> |
| X4, continued | In addition, the X4 setting enables the following functions on the Sportster modem. <ul style="list-style-type: none"> <li>• Adaptive Dialing (HUNT)—The modem attempts to use tone dialing, and if that doesn't work, it reverts to rotary (pulse) dialing.</li> <li>• Wait for Another Dial Tone (W)—The modem halts dialing until it detects another dial tone.</li> <li>• Wait for an Answer (@)—The modem does not continue dialing until it detects 5 seconds of silence on the line.</li> <li>• Fast Dial—The modem dials immediately after detecting a dial-tone, instead of waiting the normal 2 seconds set in register S6.</li> </ul>                                                                                                                                                                         |

In addition to the initialization string, the functions described in [Table 4-2](#) are other necessary parameters that need to be set on each modem. On the Sportster, these are controlled by dip switches. These parameters can be set on other modems using dip switches or within the initialization string.

**Table 4-2 US Robotics Sportster additional settings.**

| Function             | Sportster Dip Switch <sup>1</sup> | Equivalent AT Command | Description                                                                                                                            |
|----------------------|-----------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Display result codes | 3 (on)                            | no equivalent         | Enables result codes to display to our hardware.                                                                                       |
| Auto answer          | 5 (on)                            | S0=0                  | Turns the modem's auto answer function to OFF. Auto answer is not required because the JACE picks up the phone when the call comes in. |
| Smart mode           | 8 (on)                            | no equivalent         | Enables recognition of AT command set.                                                                                                 |

1. Dip switches in the on position are flipped down.

For proper operation of your modem with our hardware, you must provide functionality in your initialization string equivalent to the settings referenced in the two tables above.

## About the AT Command Set

The AT command set is industry-standard command language used to communicate with the modem. Sometimes this is referred to as the Hayes command set, because Hayes Microcomputer Products, Inc. developed the original language. The original command set included about 15 commands, but modern modems can support more than 250. Commands include configuring features such as data compression, diagnostics, and flow control. Manufacturers often make up their own commands for newer features. These commands are then specific to each manufacturer, so modem initialization strings need to be customized for the modem you are using.

The AT (attention modem) command is followed by one or more commands in the following formats:

**Basic Command Set**—a capital character followed by a digit. For example, **E0**.

**Extended Command Set**—an ampersand (&) and a capital character followed by a digit. For example, **&A1**. Note that **A1** is different from **&A1**.



**Note**

For either set, if the capital letter in the command is not followed by a number, the number implied is 0. For example, **ATE** is equivalent to **ATE0**. **AT&A** is equivalent to **AT&A0**.

**Register Commands**—Commands are in the form **Sr=n** where **r** is the number of the register to be changed and **n** is the new value that is being assigned. The S-registers are used to set various timing parameters and to redefine selected ASCII characters and other configuration options. For example, **S0=0** disables auto answer on the modem.

Settings made via AT commands are automatically reused by the modem until another command is received to change them, or the modem is turned off. The commands in the initialization string are used to set the parameters on startup.

## Enabling the JACE-4 Modem (Internal or External)

The JACE-4 has two serial ports (one RS-232 and one RS-485) and one optional on-board 56k modem. However, only two of these three serial channels can be active at any one time. By default, the serial ports are enabled rather than the modem. When shipped, COM1 is assigned to the RS232 port and COM2 is assigned to the RS485 port. If you use an external modem, you can leave the RS-232 port at COM1, or reconfigure it to be COM2. Changes to these assignments can be made using the release 2.3 of the Admin Tool.

If you have purchased the internal modem and want to enable it, you must enable the modem in the place of one of the two serial ports. The internal modem must be assigned to COM2.

You can choose from one of the following options for configuring your serial ports:

**Table 5 Serial port configuration options.**

|                           |                        |
|---------------------------|------------------------|
| <b>Option 1 (default)</b> | COM1=232<br>COM2=485   |
| <b>Option 2</b>           | COM1=232<br>COM2=MODEM |
| <b>Option 3</b>           | COM1=485<br>COM2=MODEM |

Use the following steps to configure the serial ports.

### Procedure 4-1 Configuring JACE-4 serial ports.

- 
- Step 1** Open release 2.3 of the Admin Tool and connect to the JACE-4.
- Step 2** Click the **Network Settings** tab.
- Step 3** On the Network Settings tab, click **Edit Port Properties**.

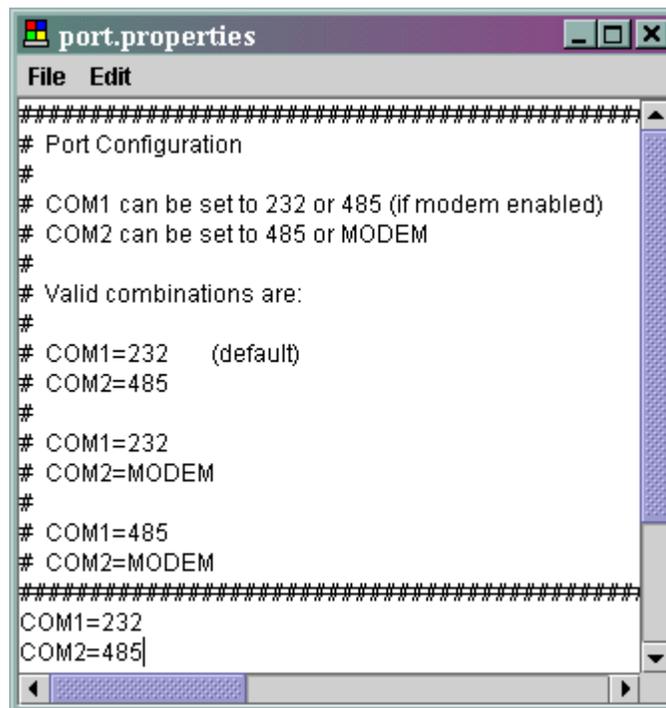


#### Notes

- If you cannot see the **Port Properties** button, maximize the Admin Tool window. If you are using the Admin Tool within the JDE, you may also have to contract the left pane to see the button.
  - The **Port Properties** button is available in Niagara release 2.3 or later. If you are not running release 2.3 on your PC, then either upgrade to that release or contact Systems Engineering for information on how to update the file.
- 

The port.properties file opens in a text editor (see [Figure 4-4](#)).

Figure 4-4 port.properties file opened for editing.



**Step 4** Make any changes to the text of the file, using any of the options from [Table 5](#).

**Step 5** From the file menu, choose **File > Close**.

If you made any changes, you are prompted to save them, otherwise the window closes.

**Step 6** If prompted to save your changes, click one of the following:

- **Yes** to save your changes. The file saves and the window closes.
- **No** to discard your changes. The window closes.
- **Cancel** to return to the editing window, then refer to [Step 4](#).

**Step 7** Reboot the JACE.

## Attaching an External Modem

Both the JACE-4 and JACE-5 have one or more DTE serial ports. This means that, in order to attach a modem (which is a DCE device), you need to use a serial cable that is pinned straight through.

### JACE-5

With the JACE-5 you use a standard serial cable with a DB-9 female connector on one end, and typically, a DB-25 male connector on the other end. Connect the DB-9 end of the cable to the serial port on the JACE-5 and the DB-25 end to the modem.

**Tip**

Attaching a PC to COM1 requires a null modem cable. If you attach the modem to COM2 you will not have to re-cable if you ever need to access the JACE through COM1 (For instance, if you use Hyperterminal. For details, see the “[Hyperterminal](#)” section on page 2-7).

**JACE-4**

For a JACE-4, you need to use an 8-wire flat silver satin stranded cable with RJ-45 connectors on both ends. Connect this cable to an adapter that converts RJ-45 to DB-9 and has been pinned out to our specifications. Connect this adapter to a standard DB-9 female to DB-25 male adapter (or adapter cable) and connect that to the modem.

For more information about connecting DCE devices to our DTE serial ports (including how to pin out the RJ-45 to DB-9 adapter), see the “[About Serial and Null Modem Cables and Adapters](#)” section on page 2-12.

## Configuring the Software

Configuring the software is a two step process. First, you use the Admin Tool to edit the ras.properties file. Then you use the Admin Tool to enable dial-in for those users who are allowed to dial into the JACE.

### About the ras.properties File

The ras.properties file is used to both configure modems and enable the direct dial function on the JACE-4/5. RAS stands for remote access service. Each parameter in this text file is listed on a separate line with an equal sign (=) followed by a value (<parameter>=<value>). Parameters can be preceded by the # sign, which disables (comments out) the parameter. You can remove the # to enable the parameter. [Example 4-1](#) shows the typical format of these parameters.

**Example 4-1 Parameter format in ras.properties file.**

```
rasEnable=false
rasMode=directDial
#dialOutOnly=false
```

Options in this file that effect direct dial are listed in [Table 4-1](#), along with valid and default values, and a description.

Table 4-1 Parameters of the ras.properties file used to configure direct dial.

| Section                        | Parameter   | Valid Values and Default Values (in Bold)                                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties             | rasEnable   | true<br><b>false</b>                                                                                                          | Change this to true to enable RAS for this JACE-4/5. The modem will not accept calls when this setting is false. In addition, when this is false, the JACE will not attempt to initialize any attached modem.<br><br><b>Note:</b> When using release 2.3, make sure to only set this to true when you have a modem installed or attached. Otherwise the JACE may be slow to boot. For an explanation, see the <a href="#">initFailLogOnly</a> parameter.                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                | rasMode     | <b>directDial</b><br>captiveISP                                                                                               | Use direct dial for this function. Captive ISP mode is discussed in <a href="#">Chapter 5, "Connecting to an ISP"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                | dialOutOnly | true<br><b>false</b>                                                                                                          | Set this to true and the JACE will not accept incoming calls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| General Properties             | remoteAddr  | any valid IPv4 address in dotted decimal notation<br><b>192.168.1.111</b>                                                     | The IP address that is used by the remote machine dialing into the JACE.<br><br>This address should <b>not</b> be: <ul style="list-style-type: none"> <li>on the same network as the address used to configure the JACE with the Admin Tool (its LAN IP address).</li> <li>on any network reachable by the JACE through its LAN IP address (if the JACE is also connected to a LAN).</li> <li>on any network reachable by the dial-in host through its LAN IP address (if the dial-in host is connected to a LAN).</li> </ul> This address should be: <ul style="list-style-type: none"> <li>an IP address on the same network as the localAddr parameter.</li> </ul> Setting up the address this way creates a unique network for dial-up between the JACE and its dial-in host. This reduces the threat of packets being routed the wrong way due to address conflicts.     |
|                                | localAddr   | any valid IPv4 address in dotted decimal notation<br><b>when parameter not listed or disabled, defaults to LAN IP address</b> | The IP address that the JACE should use when talking to the dialed-in host.<br><br>This address should <b>not</b> be: <ul style="list-style-type: none"> <li>on the same network as the address used to configure the JACE with the Admin Tool (its LAN IP address).</li> <li>on any network reachable by the JACE through its LAN IP address (if the JACE is also connected to a LAN).</li> <li>on any network reachable by the dial-in host through its LAN IP address (if the dial-in host is connected to a LAN).</li> </ul> This address should be: <ul style="list-style-type: none"> <li>an IP address on the same network as the remoteAddr parameter.</li> </ul> Setting up the address this way creates a unique network for dial-up between the JACE and its dial-in host. This reduces the threat of packets being routed the wrong way due to address conflicts. |
| Modem Configuration Properties | device      | COM1<br><b>COM2</b>                                                                                                           | The COM port used by the modem. If using the JACE-4 internal modem, this should remain at COM2. If using an external modem with the JACE-4, this should match the serial port assignment of the RS-232 port as listed in the port.properties file (see <a href="#">"Enabling the JACE-4 Modem (Internal or External),"</a> page 4-10).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table 4-1 Parameters of the ras.properties file used to configure direct dial. (continued)

| Section                                   | Parameter       | Valid Values and Default Values (in Bold)                                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modem Configuration Properties, continued | baudrate        | <b>57600</b><br>48800<br>36600<br>19200                                                                                                                                                                     | The initial baud rate to use between the JACE and the modem. In most cases you will not have to change this parameter.                                                                                                                                                                                                                                                                                                                                                                             |
|                                           | initString      | depends on modem<br><ul style="list-style-type: none"> <li><b>JACE-5—AT&amp;F1E0X4</b> (USR Sportster)</li> <li><b>JACE-4—ATE0Q0V1X4&amp;D2&amp;K3IN3%C2&amp;C1&amp;Q5W2</b> (internal Cermetek)</li> </ul> | The modem-specific initialization string sent to the modem when the JACE boots. It sets options required by our hardware (see the “ <a href="#">About Pre-configured Modems</a> ” section on page 4-7).<br>Initialization string for the Zoom External V.90 Dualmode Faxmodem— AT&FE0S0=0                                                                                                                                                                                                          |
|                                           | updateNvRamCmd  | depends on modem<br><ul style="list-style-type: none"> <li><b>AT&amp;W0</b> (USR Sportster)</li> </ul>                                                                                                      | Modem specific command used to save the initialization string to <b>O</b> so it is available to initialize the modem if the modem reboots and the JACE does not.                                                                                                                                                                                                                                                                                                                                   |
|                                           | updateNvRamFlag | <b>false</b><br>true                                                                                                                                                                                        | Set to true to save the initialization string to NVRAM during the next boot. This flag must be manually set to true each time <b>initString</b> is changed. The JACE will automatically set this back to false after the NVRAM has been successfully updated. This prevents unnecessary writes to modem NVRAM.                                                                                                                                                                                     |
|                                           | initFailLogOnly | <b>false</b><br>true<br><br><b>Note:</b> Supported in release 2.3 or later.                                                                                                                                 | When <b>rasEnable=true</b> , and this parameter is set to false, and the JACE is rebooted, the JACE reboots up to three times trying to initialize the modem. If the modem is not initialized by the third time, the following message is sent to the Admin Tool’s event log, and dial up is disabled:<br><br><code>Disabling dialup. Too many init failures.</code><br>When set to true, the JACE will not reboot if the modem doesn’t initialize, but will only send a message to the event log. |
| Miscellaneous Properties                  | pppDebug        | <b>false</b><br>true                                                                                                                                                                                        | Set to true to see dial-up troubleshooting information. This information is written to the VxWorks target shell, and is accessible via direct connect (Hyperterminal) or over a LAN connection (Telnet).                                                                                                                                                                                                                                                                                           |
|                                           | modemDebug      | <b>false</b>                                                                                                                                                                                                | Set to true to see dial-up troubleshooting information. This information is written to the VxWorks target shell, and is accessible via direct connect (Hyperterminal) or over a LAN connection (Telnet).<br><br><b>Note:</b> Neither of these parameters is listed in the ras.properties file but you can add them.                                                                                                                                                                                |
|                                           | rasDebug        | true                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring ras.properties for Direct Dial

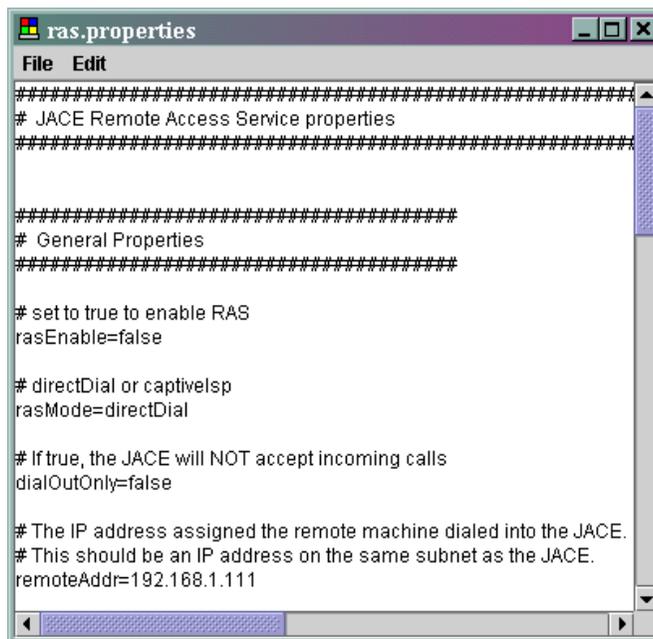
Use the following steps to configure the JACE-4/5 for direct dialing.

### Procedure 4-2 Configuring the JACE-4/5 for direct dialing.

- Step 1** Click the **Network Settings** tab.
- Step 2** Click **Edit Modem Properties**.

The ras.properties file is opened for editing ([Figure 4-5](#)).

Figure 4-5 ras.properties file opened for editing.



```

ras.properties
File Edit
#####
JACE Remote Access Service properties
#####

#####
General Properties
#####

set to true to enable RAS
rasEnable=false

directDial or captivelsp
rasMode=directDial

If true, the JACE will NOT accept incoming calls
dialOutOnly=false

The IP address assigned the remote machine dialed into the JACE.
This should be an IP address on the same subnet as the JACE.
remoteAddr=192.168.1.111

```

**Note**

The first time you view the ras.properties file, it contains remarks explaining each setting. The remark lines are preceded by a pound sign (see the example above). After saving the file, the remarks are stripped out and any future edits of the file will not contain the remarks.

**Step 3** Edit the file using the information in [Table 4-1](#) as a guide. At a minimum, you must configure the following items:

**General Properties**

- **rasEnable**—change **false** to **true**.
- **remoteAddr**—set this as described in the **Description** column of [Table 4-1](#).
- **localAddr**—set this as described in the **Description** column of [Table 4-1](#). If the parameter is missing, add it in the form `localAddr=<value>`.

**Modem Configuration Properties**

- **device**—change to **COM1** if your modem is attached to that port.
- **initString**—change if you are using a modem other than those that we have pre-configured.

**Tip**

The Sportster and Zoom initialization strings and update NVRAM commands are pretty standard. Consider trying them with your modem to see if they work for you.

- **updateNvRamCmd**—change if you are using a modem other than those that we have pre-configured.

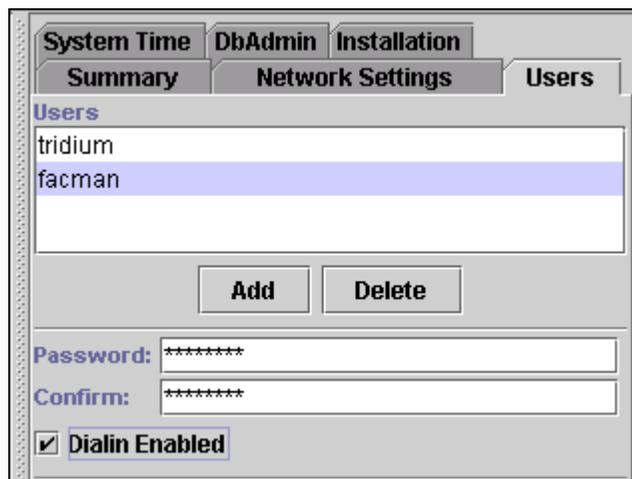
- `updateNvRamFlag`—change **false** to **true** if you have updated the initialization string.
- Step 4** From the file menu, choose **File > Close**.
- If you made any changes, you are prompted to save them, otherwise the window closes.
- Step 5** If prompted to save your changes, click one of the following:
- **Yes** to save your changes. The file saves and the window closes.
  - **No** to discard your changes. The window closes.
  - **Cancel** to return to the editing window, then refer to [Step 4](#).
- Step 6** Reboot the JACE.

**Enabling Dial-in** Use the following steps to enable dial-in for any user who will connect to this host via the modem.

**Procedure 4-3 Enabling dial-in for users connecting to this host.**

- Step 1** Using the **Admin Tool**, open the JACE-4/5.
- Step 2** Enable dial-in for any users who will be allowed to connect to this JACE via the modem:
- a. Click the **Users** tab.
  - b. Click any existing user.
  - c. Click **Dialin Enabled**. A check appears in the box ([Figure 4-6](#)).
  - d. Click **Apply**.
  - e. Repeat for any additional users.

**Figure 4-6 User enabled for dial-in.**



# Configuring Direct Dial on the JACE-NP

Configuring direct dial on the JACE-NP consists of three major steps:

- [Installing and Configuring Modems](#)
- [Configuring the RAS Software](#)
- [Granting Dial-in Permissions](#)

## Installing and Configuring Modems

You can purchase an internal modem when ordering a JACE-NP, or you can attach an external one to either of the RS-232 serial ports. When you order an internal modem with a JACE-NP you must also buy the upgrade to the full version of NT as the embedded version will not work with the internal modem.



### Caution

Do not add your own internal modem to a JACE-NP. This invalidates your warranty.

## Supported Modems

When shipped with an internal modem, a driver for that modem is configured in the NT OS for COM3. When no internal modem is purchased, a driver for the U.S. Robotics 56K Fax External modem is configured on COM1.

If you choose not to use our supplied internal modem, or the pre-configured default, you can use any modem that provides a driver for Windows NT 4.0.

## Installing an External Modem

To install the modem, connect a standard serial cable to the DB-9 male serial port of your choosing on the JACE (either COM1 or COM2). Attach the other end of the serial cable to the DB-25 male connector on the modem.



### Note

The JACE-NP does not support USB-connected modems.

## Installing the Modem Driver

Many modem drivers are provided with the Windows NT 4.0 OS. However, if you are using a modem driver that is not available in the OS, you must load the driver. Since the JACE-NP has no floppy disk to load the driver, your JACE-NP must be attached to a LAN. The LAN provides the access method to the driver file.

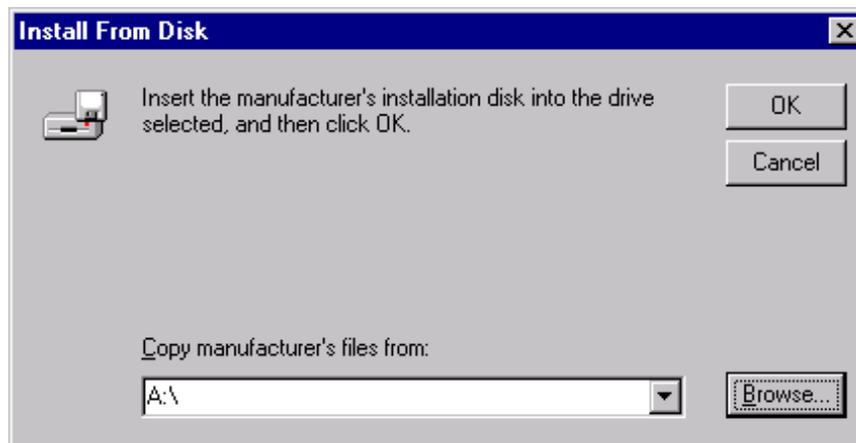
Use the following steps to add a modem driver to a JACE-NP.

### Procedure 4-4 Installing a modem driver on the JACE-NP.

- Step 1** If you are installing the driver on a JACE-NP with Embedded NT, access the Windows NT desktop with NetMeeting (see “[NetMeeting](#),” page 2-2). Otherwise, attach a keyboard, monitor, and mouse to access the desktop.

- Step 2** From the Windows NT 4.0 taskbar, open the Control Panel by choosing **Start > Settings > Control Panel**.
- Step 3** Double-click the **Modems** icon to open it.
- Step 4** Click **Add**.
- Step 5** In the **Install New Modem** dialog box, click the **Don't detect my modem** box, and click **Next**.
- Step 6** If your modem manufacturer and model are listed (Figure 4-9), choose them from the list and click **Next**. Otherwise, click **Have Disk** and do the following:
- a. In the **Install from Disk** dialog box, click **Browse** (Figure 4-7).

Figure 4-7 Install From Disk dialog box.



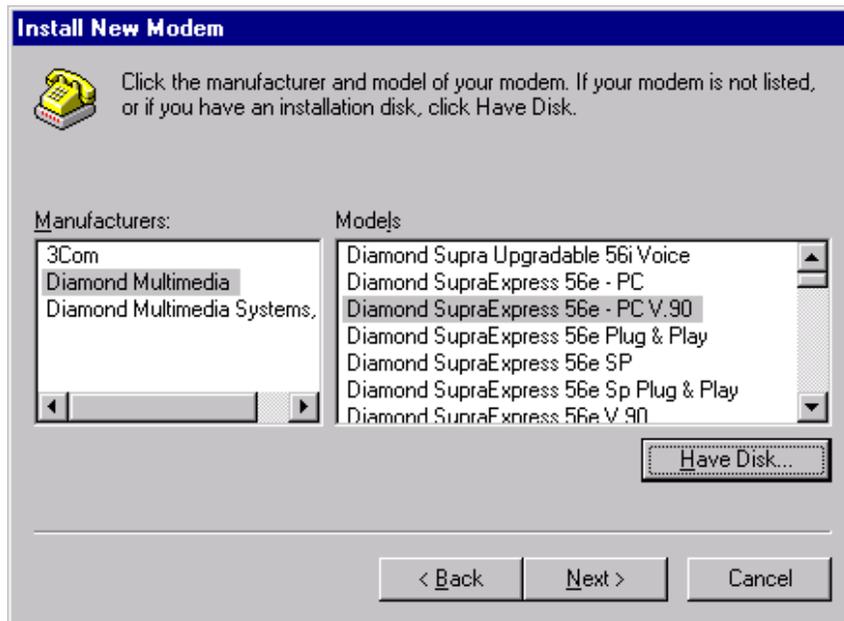
- b. Click **OK** on the error message about A:\ having been removed. The JACE-NP does not have an A: drive.
- c. In the **Locate File** dialog box (Figure 4-8), browse the network to locate the modem driver (typically an .inf file), and click **Open**.

Figure 4-8 Locate File dialog box.



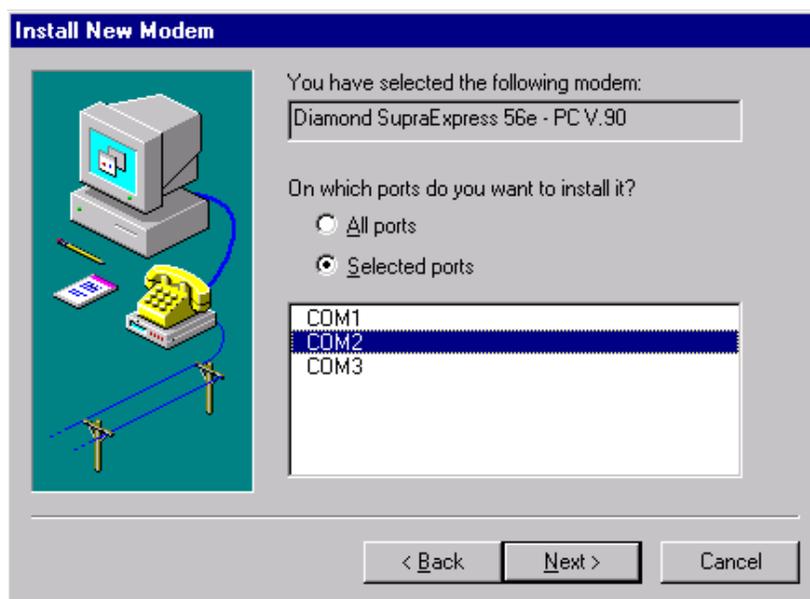
- d. Click **OK**.
- e. In the **Install from Disk** dialog box (Figure 4-7), click **OK** to copy the manufacturer's file from the network location.
- f. In the **Install New Modem** dialog box (Figure 4-9), choose the model of your modem and click **Next**.

Figure 4-9 Install New Modem dialog box.



- Step 7** On the port selection dialog box (Figure 4-10), click the COM port on which you have installed the modem, and click **Next**.

Figure 4-10 Port selection dialog box.



- Step 8** Click **Finish**.
- Step 9** On the **Modems Properties** dialog box, click **Close**.
- Step 10** Reboot the JACE-NP by choosing **Start > Shutdown**, then choosing **Yes**.
- 

## Configuring the RAS Software

On the JACE-NP, dialing into and out of the JACE-NP is a function of NT's Remote Access Server (RAS). RAS is an optional Windows NT 4.0 service that allows users to log into an NT-based LAN using a modem, X.25 connection, or WAN link. RAS works with several of the most popular network protocols including TCP/IP, IPX, and NetBEUI.

RAS is pre-installed on the JACE-NP. However, setting it up is a two step process:

- [Configuring RAS](#)
- [Starting RAS](#)

### Configuring RAS

Use the following steps to configure RAS on the JACE-NP.

#### Procedure 4-5 Enabling RAS on a JACE-NP.

---

- Step 1** If you are installing the driver on a JACE-NP with Embedded NT, access the Windows NT desktop with NetMeeting (see "[NetMeeting](#)," page 2-2). Otherwise, attach a keyboard, monitor, and mouse to access the desktop.
- Step 2** From the Windows NT 4.0 taskbar, open the Control Panel by choosing **Start > Settings > Control Panel**.
- Step 3** Double-click the **Network** icon to open it.
- Step 4** Click the **Services** tab.
- Step 5** Click **Remote Access Service** and click **Properties** ([Figure 4-11](#)).  
The **Remote Access Setup** dialog box opens ([Figure 4-12](#)).

Figure 4-11 RAS properties.

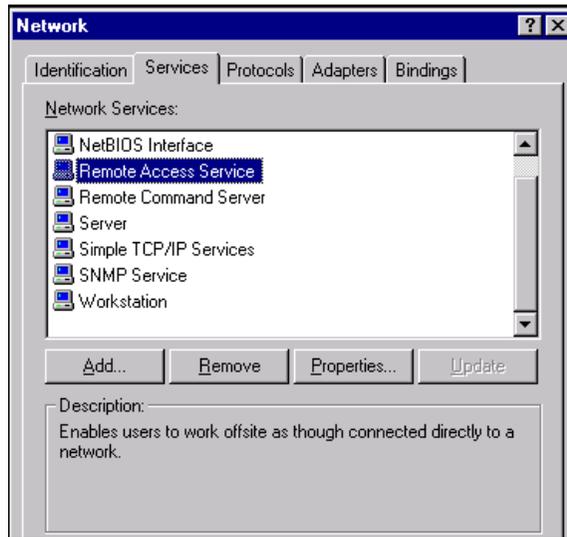
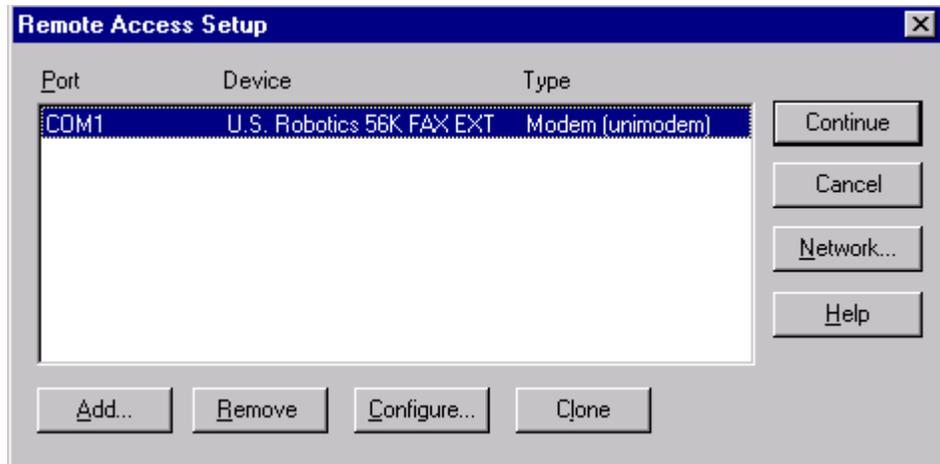
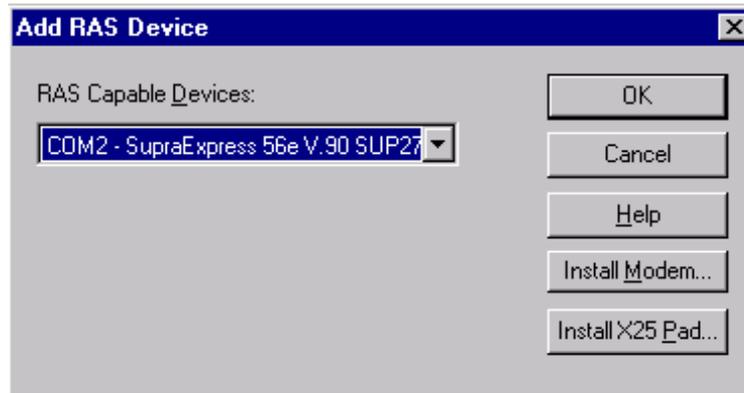


Figure 4-12 Remote Access Setup dialog box.



- Step 6** If your modem is listed in the dialog box, click **Configure**. Otherwise, do the following to add your modem:
- Click **Add**.
  - In the **Add RAS Device** dialog box (Figure 4-13), click **OK**. Your modem is added to RAS and is now available to set up.

Figure 4-13 Add RAS Device dialog box.



- c. In the **Remote Access Setup** dialog box (Figure 4-12), choose your modem and click **Configure**.

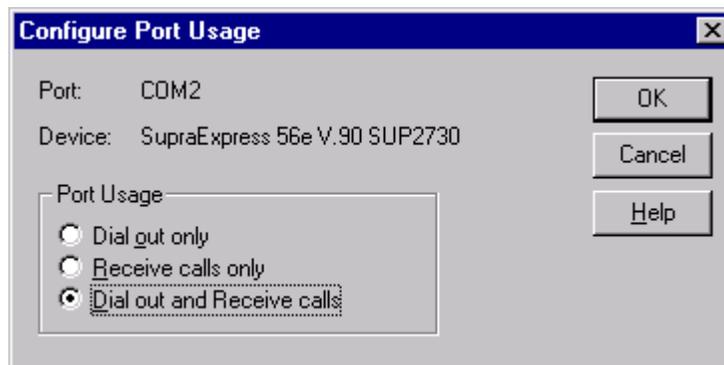
**Step 7** On the **Configure Port Usage** dialog box (Figure 4-14), ensure that your modem is set up to **Dial out and Receive calls**, then click **OK**.

Selecting both dial-out and dial-in capability allows the JACE controller to be accessed from a remote client as well as dial out to a Web Supervisor for the purpose of archiving alarms and trend data.



**Note** In Windows NT Embedded only one port can receive calls. If you are adding an additional modem and want it to receive calls, change the pre-configured modem to dial out only.

Figure 4-14 Configure Port Usage dialog box.

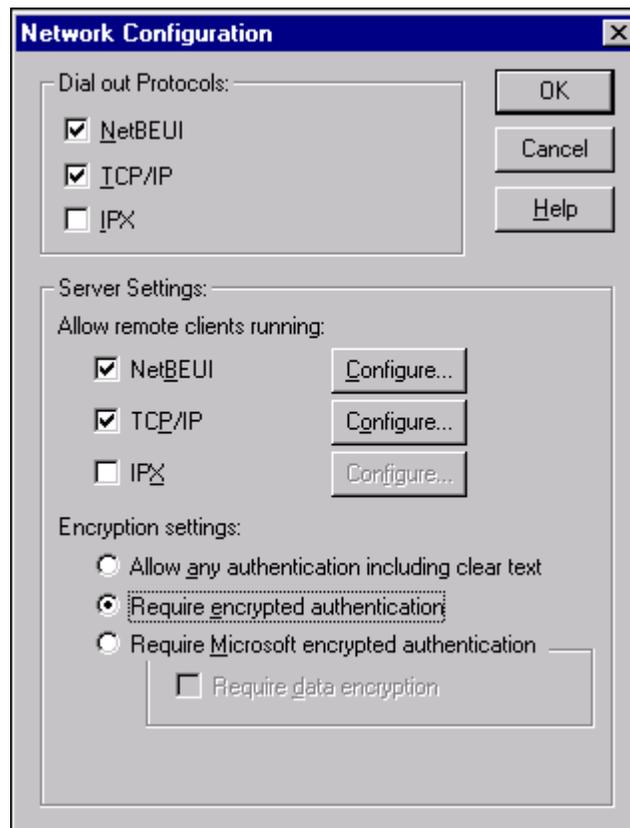


**Step 8** On the **Remote Access Setup** dialog box (Figure 4-12), click **Network**.

**Step 9** In the **Network Configuration** dialog box (Figure 4-15), configure the following settings:

- Ensure that **TCP/IP** is checked in both the **Dial out Protocols** and **Server Settings** sections.
- In the **Encryption settings** section, click **Require encrypted authentication**.

Figure 4-15 Network Configuration dialog box.

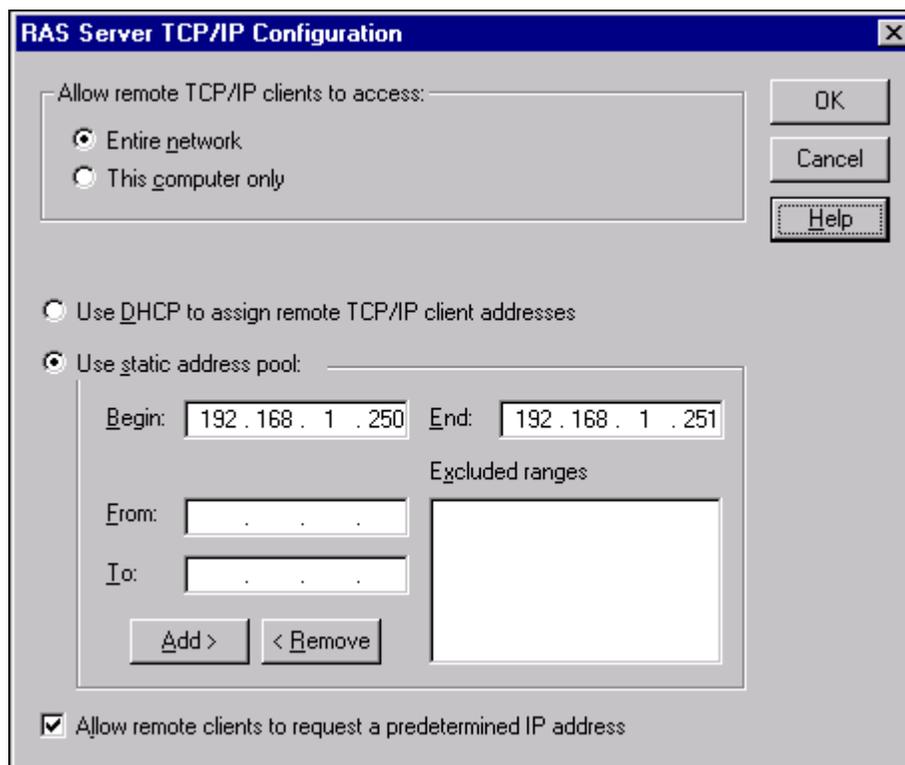


**Step 10** In the **Server Settings** section, click the **Configure** button next to **TCP/IP**.

**Step 11** In the **RAS Server TCP/IP Configuration** dialog box (Figure 4-16), configure the following options:

- **Allow remote TCP/IP clients to access**—if you want the dial-in client to only manage this JACE-NP, choose **This computer only**. If, instead you want the dial-in client to access other resources on the network, use **Entire network**.
- **Use static address pool**—Specify two IP addresses, one for the JACE-NP, and one for any client that will dial-in. These addresses:
  - must be on the same subnet as the LAN IP address of the JACE-NP (if you want the remote client to be able to access other resources on the network).
  - must not duplicate the LAN IP address of the JACE-NP.
  - must not duplicate any address already in use by other network hosts.
- **Allow remote clients to request a predetermined IP address**—click the check box.

Figure 4-16 RAS Server TCP/IP dialog box.



- Step 12** To save your changes:
- On the **RAS Server TCP/IP Configuration** dialog box, click **OK**.
  - On the **Network Configuration** dialog box, click **OK**.
  - On the **Remote Access Setup** dialog box, click **Continue**.
  - On the **Network** dialog box, click **Close**.

The Windows NT setup wizard finalizes the set up of the service.

## Starting RAS

Once RAS has been configured on the JACE controller, the service needs to be started, then configured to start automatically each time the JACE controller is restarted.

### Procedure 4-6 Starting RAS.

- Step 1** In the Windows **Control Panel**, double-click the **Services** icon.  
A list of installed services appears.
- Step 2** In the **Services** dialog box, scroll down and click **Remote Access Server**, then click **Start**.  
Verify that the service starts successfully (the status changes to **Started**).

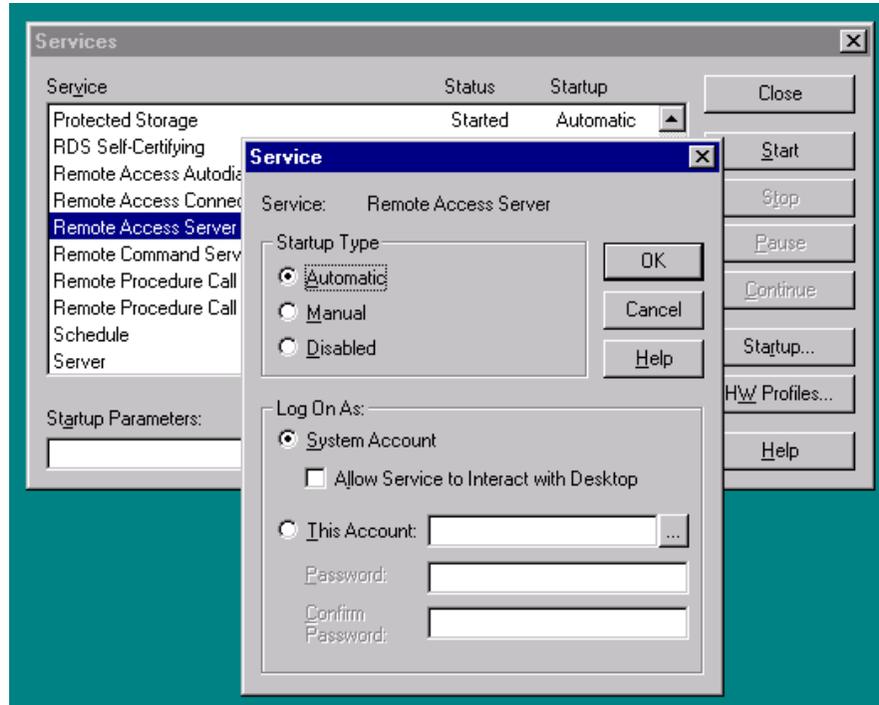


**Note** In order to start the service, your RAS must be configured and your modem must be turned on.

**Step 3** With **Remote Access Server** selected, click **Startup**.

**Step 4** Click the radio button next to **Automatic**, then click **OK** (see [Figure 4-17](#)).

**Figure 4-17** Starting RAS.



**Step 5** On the Services dialog box, click **Close** to save your changes.

## Granting Dial-in Permissions

If any host is going to connect to RAS on the JACE controller you must grant the connecting user dial-in permissions. You do this on the Users tab of the Admin tool. For complete instructions, refer to the [“Enabling Dial-in”](#) section on page 4-16.

## Configuring Direct Dial on an Engineering PC

Configuring direct dial on an engineering PC (be it a Web Supervisor or a Technician PC) consists of three major steps:

- [Installing and Configuring Modems](#)

- [Installing and Configuring the RAS Software](#)
- [Granting Dial-in Permissions](#)

## Installing and Configuring Modems

### Supported Modems

You can use any modem which provides a driver for the version of the OS you are running on the PC.

### Installing an External Modem

To install the modem, connect a standard serial cable to the male serial port of your choosing on the PC. Attach the other end of the serial cable to the DB-25 male connector on the modem.

**Note**

---

Alternately, if you are using Windows 2000 as your operating system, you can attach a USB modem. Windows NT 4.0 does not support USB-connected devices.

---

### Installing the Modem Driver

Many modem drivers are provided with the Windows OS. However, if you are using a modem driver that is not available in the OS, you must load the driver. Use the following instructions to load the driver onto your engineering PC.

#### Windows NT 4.0

These instructions are included in the configuration of the JACE-NP. See the [“Installing the Modem Driver”](#) section on page 4-17.

#### Windows 2000

---

**Procedure 4-7 Installing the modem driver in Windows 2000.**

---

- Step 1** On the taskbar click **Start > Settings > Control Panel**.
- Step 2** Click **Phone and Modem Options**.
- Step 3** Click the **Modems** tab.

Figure 4-18 Phone and Modem Options dialog box.



**Step 4** Continue with [Step 4](#) in [Procedure 4-4](#) “Installing a modem driver on the JACE-NP.”

## Installing and Configuring the RAS Software

Just as on the JACE-NP, dialing into and out of an engineering PC is a function of NT’s Remote Access Server (RAS). RAS is an optional Windows NT 4.0 or 2000 service that allows users to log into an NT-based LAN using a modem, X.25 connection, or WAN link. RAS works with several of the most popular network protocols including TCP/IP, IPX, and NetBEUI.

Installing and configuring RAS on an engineering PC consists of the following steps:

- [Installing the RAS Software \(Windows NT 4.0 only\)](#)
- [Configuring RAS](#)
- [Starting RAS \(Windows NT 4.0 only\)](#)

### Installing the RAS Software (Windows NT 4.0 only)

Install the RAS service on a Windows NT 4.0 host as follows.



**Note** Proper operation of RAS requires a functional installation of Windows NT Service Pack 4. Ensure that Service Pack 4 (or later) has been installed on your computer before attempting to install this service.

---

**Procedure 4-8 Installing RAS on a Windows NT 4.0 host.**

---

- Step 1** On the taskbar of the engineering PC, click **Start > Settings > Control Panel**.
- Step 2** Double-click the **Network** icon, then click the **Services** tab.  
If the Remote Access Service is not listed, continue as follows to install the service. Otherwise, you are finished.
- Step 3** In the Network dialog, click the **Add** button.  
Windows builds the list of available services.
- Step 4** Scroll down and click **Remote Access Service**, then click **OK**.
- Step 5** If the Windows NT setup wizard finds the Windows NT files, click **OK** to proceed. Otherwise, locate the RAS installation files and specify that location in the Windows setup dialog and click **Continue**.



**Note** Depending on your installation, the RAS files may be located in the c:\i386 directory. If you cannot find them there look on the Windows NT 4.0 installation CD in the \i386 directory. However, if you install from the original CD you must re-apply the appropriate NT service pack when finished installing RAS.

- Step 6** In the **Add RAS Device** dialog box, choose the modem you installed in the previous procedure.
- 

## Configuring RAS

After you have installed RAS, you must configure it. Use the following instructions to configure RAS on Windows NT 4.0 or the equivalent feature on Windows 2000.

### Windows NT 4.0

These instructions were provided in the JACE-NP setup section. See [“Configuring RAS,”](#) page 4-20.

## Windows 2000



### Notes

- In order to fully configure RAS, you must log into the Windows 2000 host with administrative privileges.
- It is possible for the Windows 2000 domain administrator to override any RAS settings you make with a system policy that restricts these settings. Check with the domain administrator to determine if restrictive policies are in effect for the site.

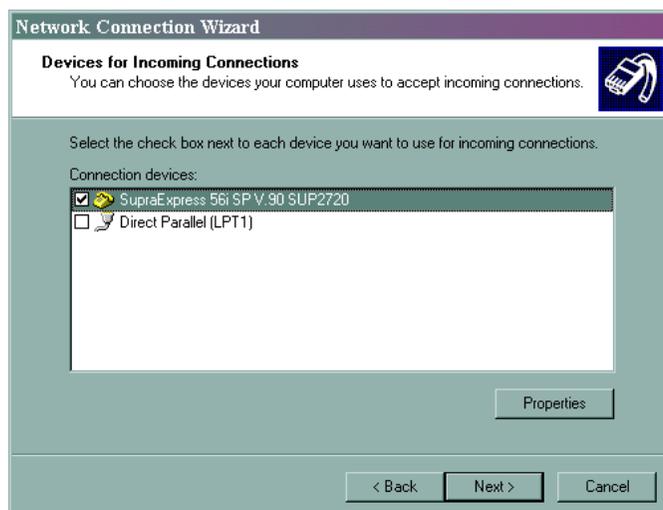
### Procedure 4-9 Configuring dial-in on Windows 2000.

- Step 1** On the Windows 2000 taskbar, select **Start > Settings > Control Panel**.
- Step 2** Double-click **Network and Dial-up Connections** then double-click **Make New Connection**. The Network Connection Wizard starts.
- Step 3** Click **Next** on the Welcome screen.
- Step 4** Click **Accept incoming connections** and then click **Next** (Figure 4-19).

**Figure 4-19** Accepting incoming connections.



- Step 5** In the **Incoming Connections** dialog box (Figure 4-20), click the check box next to the modem you added in the “**Installing and Configuring Modems**” section. Click **Next**.

**Figure 4-20** Select device for the incoming connection.

**Step 6** In the **Virtual Private Network** dialog box, click **Next**.

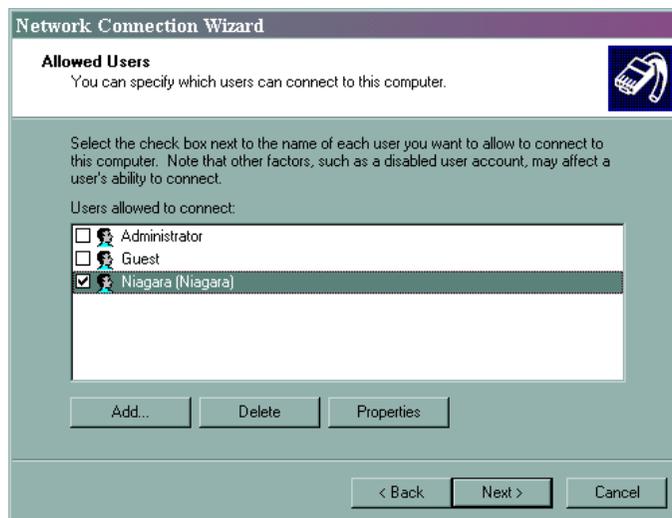


**Note** It is not necessary to set up a VPN between direct-dial hosts.

**Step 7** In the **Allowed Users** dialog box (Figure 4-21), click the check box next to any user who you want to grant permissions to dial into this computer.

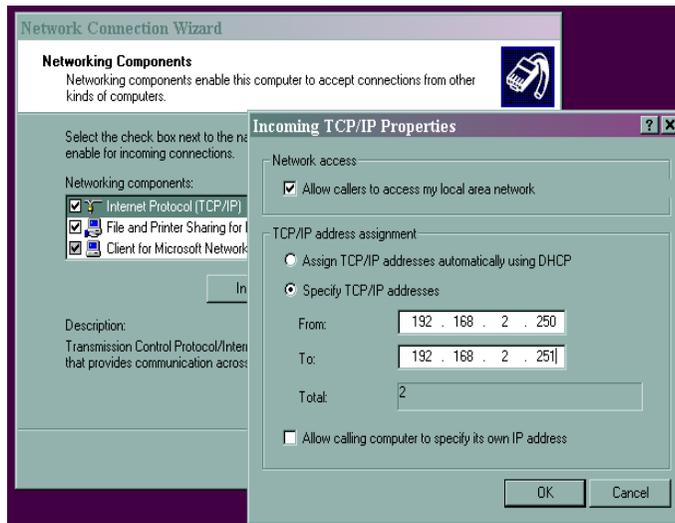


**Note** This is equivalent to granting the user dial-in permissions in the Admin Tool.

**Figure 4-21** Grant dial-in permissions.

**Step 8** On the **Networking Components** dialog box, click **Internet Protocol** and click **Properties** (Figure 4-22).

Figure 4-22 Set up networking components.



**Step 9** On the **Incoming TCP/IP Properties** dialog box, set up options as follows. When finished, click **OK** then **Next**.

- **Network Access**—leave this option checked if you want the host dialing in to be able to access both this host and other resources on the network.
- **TCP/IP Address Assignment**—Specify two IP addresses, one for this computer, and one for any client that will dial-in. These addresses:
  - must be on the same subnet as the LAN IP address of the JACE-NP (if you want the remote client to be able to access other resources on the network).
  - must not duplicate the LAN IP address of the JACE-NP.
  - must not duplicate any address already in use by other network hosts.

**Step 10** Click **Finish**.

## Starting RAS (Windows NT 4.0 only)

After you have installed and configured RAS, you must start the RAS service for any Windows NT 4.0 installation (the RAS service is automatically started in Windows 2000). Instructions for starting RAS were provided in the JACE-NP RAS setup section. See “[Starting RAS](#),” page 4-24.

## Granting Dial-in Permissions

If any person (or station) is going to connect to RAS on this computer, you must grant the user dial-in permissions. You may have also granted the permissions as part of the RAS setup in Windows 2000. If so, you can skip this step.

For complete instructions on setting up users for dial-in, refer to the “[Enabling Dial-in](#)” section on page 4-16.

## Using Direct Dial

Now that you have set up direct dial on your Niagara hosts, you must set up a few more things in order to use it.

If your host will be making application-initiated calls (see the “[User- versus Application-initiated Connections](#)” section on page 4-4), you must configure the station address book so it knows where to find the host with which it wants to communicate.

Making a user-initiated connection requires other configuration, and a manual process to contact the remote host.

These topics discuss using direct dial on your hosts:

- [Configuring the Station for Dial-out](#)
- [Making a User-initiated Connection from an Engineering PC](#)

## Configuring the Station for Dial-out



### Note

For most application-initiated connections, after you configure the station to find the remote host, you do not need to do anything else—the station makes the connection when it needs to. However, acknowledging alarms is different. The process is this:

1. Open the Alarm Console and acknowledge the alarm from the remote station.
2. Wait for the station to connect to the remote host.
3. Acknowledge the alarm a second time.

Failure to follow this process may result in you having to manually clear the alarm acknowledgement database.

Configure the remote host in the station’s address book, as follows:

### Procedure 4-10 Configuring the station for dial-out.

- Step 1** Using the **Java Desktop Environment (JDE)**, open the station running on the JACE-NP.
- Step 2** In the tree view, right-click the station name and choose **Go > AddressBook**.
- Step 3** Click the **Add Address** button. 
- Step 4** In the **New Address** dialog box ([Figure 4-23](#)), fill out the following information:
  - **Station Name**—The Niagara station name of the remote station. Must be unique from other station entries in the AddressBook.
  - **User Name**—An existing user account in the remote station. Specific security rights for this user are not needed.




---

**Note** Typically, a “gdp” (global data passing) user is created in each station and assigned no security rights and no (blank) password. This user is referenced in AddressBook entries in other stations.

---

- **Password**—Password for the user in the remote station. See the Note above.
- **Confirm Password**—Same password, repeated.
- **Host Address**—For a LAN connected host, this is the IP address (recommended) or hostname for the remote station's host. You must also specify the HTTP port of the remote station, if it has been changed from the default port (80). For example:

**10.10.8.21:8080**

In the case of dialup access, you can either:

- leave this field blank
- type an alternate port number, in the form **:<port\_number>**. For example, if the remote station's default HTTP has changed from the default to port 8080, you would type the following in the **Host Address** text box.

**:8080**

See also “[Impact of Changing Default Niagara Ports](#),” page 6-18.

- **Phone #**—Phone number to dial into the remote host machine.
- **Host User Name**—Logon user name for the host machine. This is the same user name you use to log in with the Admin Tool.




---

**Note** This user should have been granted dial-in permissions on the remote host. For more information, see “[Enabling Dial-in](#),” page 4-16.

---

- **Host Password**—Password for the user name above, to access the host machine.
- **Confirm Password**—Same password, repeated.
- **(Station Relationship)**—Choose the description of the remote station's relationship to this station. Typically this will be Supervisor, but it could be a Peer of another JACE is acting as this JACE's archive destination.

Figure 4-23 New Address dialog box.

Step 5 When finished filling out the new AddressBook entry, click **OK**.

## Making a User-initiated Connection from an Engineering PC

In order to contact a remote direct-dial server, you must manually initiate a connection from the engineering PC (be it a Web Supervisor or Technician PC). This would include any connections for:

- Engineering the remote station
- Reviewing web pages hosted on the remote station
- Using the Admin Tool to maintain the host

You create the connection with Windows Dial-up Networking (DUN). After you launch the connection, you use the IP address of the remote server to access the host or station database.



### Caution

The only reliable way to make a user-initiated connection is by using the following method. **Do not** use the **File > Open Dial-up (Station)** option located on the menus of either the Admin Tool or the JDE.

## Creating the DUN Connection

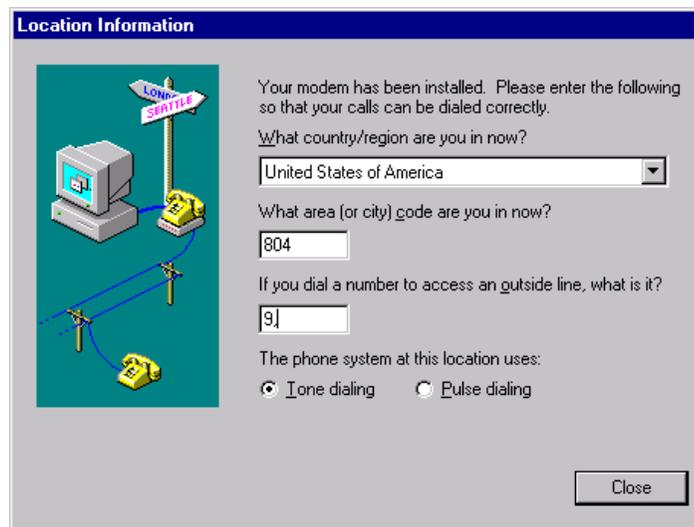
To create the DUN connection, proceed as follows.

### Windows NT 4.0

#### Procedure 4-11 Creating a DUN phonebook entry.

- Step 1** Double-click **My Computer** on the Windows NT 4.0 desktop.
- Step 2** Double-click **Dial-Up Networking**.
- Step 3** If you have not already done so, specify the local area code, dialing prefix for accessing an outside line, and other modem properties in the **Location Information** dialog box, and click **Close**.

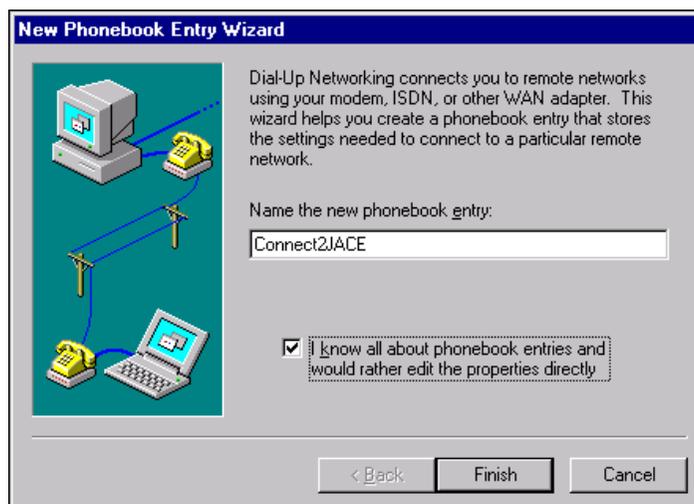
**Figure 4-24** Specifying location information for the DUN phonebook.



You are prompted to proceed (click **OK**) and you see the connection wizard.

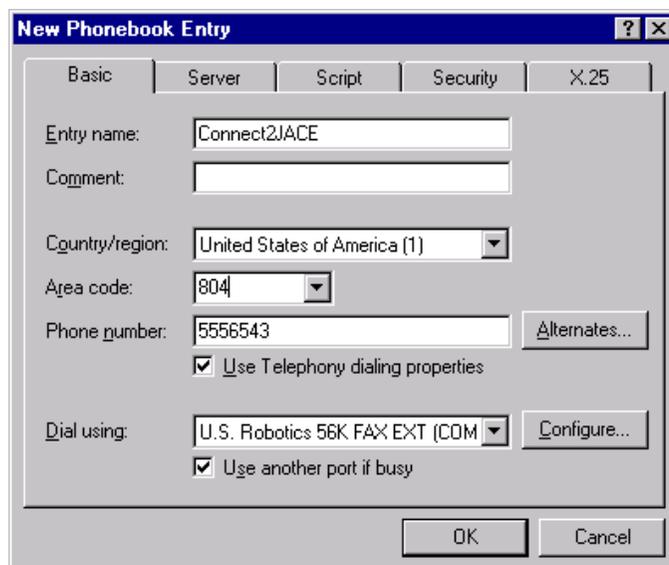
- Step 4** In the **Phonebook Entry Wizard** (Figure 4-25) do the following:
  - a. Type a name for the new phonebook entry.
  - b. Check **I know all about phonebook entries**.
  - c. Click **Finish**.

Figure 4-25 Phonebook entry wizard.



- Step 5** On the **Basic** tab (Figure 4-26) of the **New Phonebook Entry** dialog box, do the following:
- a. Check **Use Telephony dialing properties**
  - b. Type the **Area code** and **Phone number** of the host you want to dial.
  - c. Verify that the correct modem is listed in the **Dial using** section.

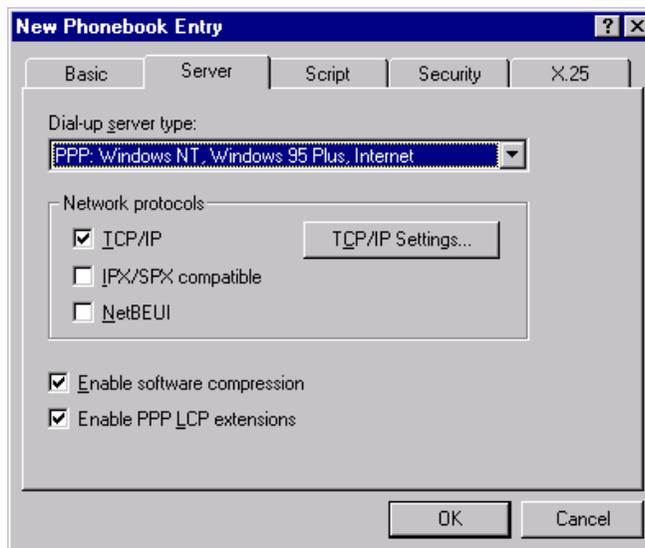
Figure 4-26 New phonebook entry Basic tab information.



- Step 6** Click the **Server** tab (Figure 4-27) and do the following:
- a. Set **Dial-up server type** to **PPP: Windows NT, Windows 95 Plus, Internet**.
  - b. Check **TCP/IP** as the **Network protocol**.
  - c. Check **Enable software compression**.
  - d. Check **Enable PPP LCP extensions**.

- e. Click the **TCP/IP Settings** button.

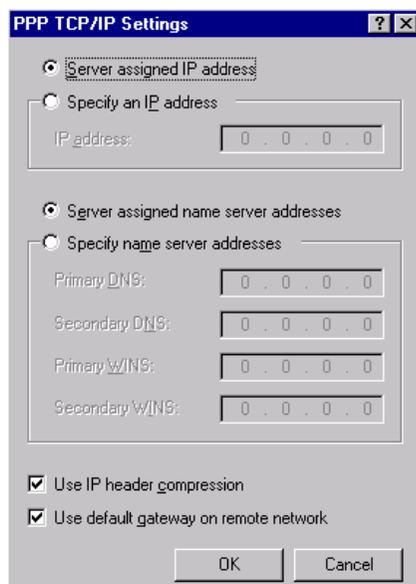
**Figure 4-27** Server tab settings.



**Step 7** On the **PPP TCP/IP Settings** dialog box (Figure 4-28), verify the following settings, then click **OK**:

- **Server assigned IP address** is selected. The PC will receive its IP address from the remote host.
- **Use IP header compression** is checked.
- **Use a default gateway on remote network** is checked.

**Figure 4-28** PPP TCP/IP settings.



You are returned to the **New Phonebook Entry** dialog box.

- Step 8** Click the **Security** tab and click the radio button next to **Accept only encrypted authentication**.
- Step 9** To save your changes:
- Click **OK** to close the **New Phonebook Entry** dialog box.
  - Click **Close** to close the **Dial-Up Networking** dialog box.

## Windows 2000

### Procedure 4-12 Creating a DUN connection in Windows 2000.

- Step 1** On the Windows 2000 taskbar, select **Start > Settings > Control Panel**.
- Step 2** Double-click **Network and Dial-up Connections** then double-click **Make New Connection**. The Network Connection Wizard starts.
- Step 3** Click **Next** on the Welcome screen.
- Step 4** Click **Dial-up to private network** and then click **Next** (Figure 4-29).

**Figure 4-29** Dial up to private network.



- Step 5** On the **Phone Number to Dial** dialog box (Figure 4-30), do the following:
- Click **Use dialing rules**.
  - Type the **Area code** and **Phone number** of the host you want to dial.
  - Click **Next**.

Figure 4-30 Phone number to dial.

- Step 6** On the **Connection Availability** dialog box, click **Next**.  
This makes the connection you are creating available to all users on this PC.
- Step 7** At the completion dialog box, do the following:
- a. Type a name for this connection.
  - b. Click **Add a shortcut to my desktop** if you want to do that.
  - c. Click **Finish**.

## Establishing the Connection

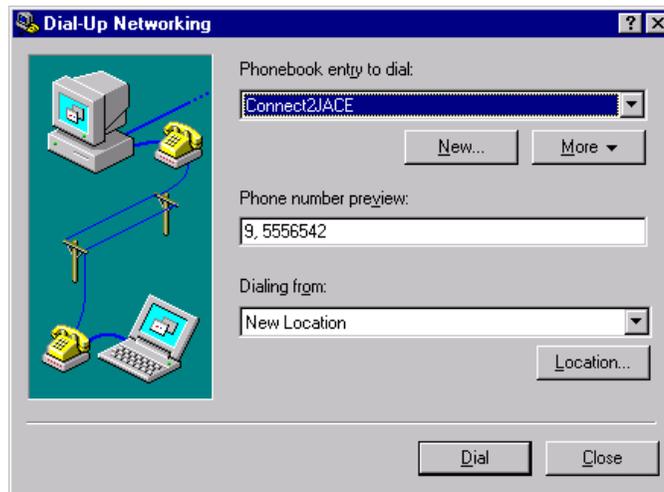
To open a connection between your PC and the remote host, proceed as follows.

### Windows NT 4.0

#### Procedure 4-13 Making the DUN connection on Windows NT 4.0.

- Step 1** Double-click the **My Computer** icon on the desktop.
- Step 2** Double-click the **Dial-Up Networking** icon.
- Step 3** Select the appropriate phone book entry, then click **Dial** (Figure 4-31).

Figure 4-31 Dial the DUN connection.



- Step 4** In the **Connect to** dialog box, type the user name and password that provides you access to the operating system running on the remote host, and click **OK**.



**Tip** This is the same user that you granted dial-in permissions to on the remote host.



**Note** You can also select the **Save Password** check box; however, if you do so, anyone who has access to your PC will have access to the host that you are dialing. This violates standard security practice.

Figure 4-32 Supply user name and password credentials for remote host.



RAS attempts to establish a connection between the modem on your computer and the modem on the remote host. Wait for the connection to be made.

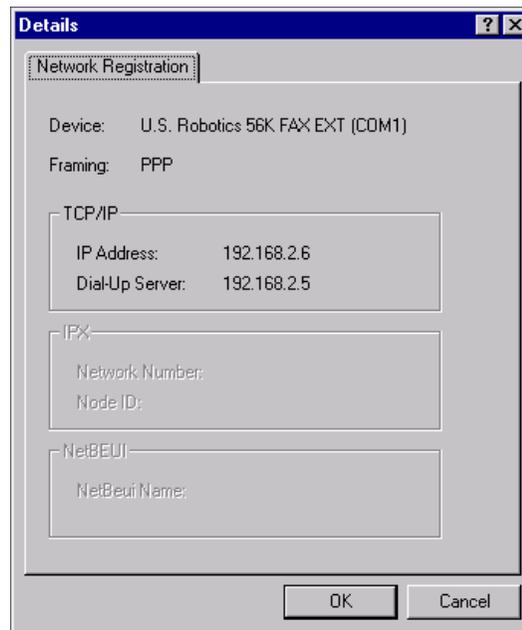
- Step 5** If a **Connection Complete** dialog box is displayed, click **OK** to proceed.
- Step 6** With the connection made, right-click the **Dial-Up Networking Monitor**  on the taskbar and click **Open Dial-up Monitor**.

The **Dial-Up Networking Monitor** allows you to check the status of the connection and to discover the IP address assigned to your machine and that of the remote server.

- Step 7** With the Dial-Up Networking Monitor displayed, click the **Details** button (Figure 4-33).

The **IP Address** field displays the address assigned to your machine for this connection. The **Dial-Up Server** field displays the IP address of the remote server (make note of this address; you will use it later).

**Figure 4-33** TCP/IP connection details.



With the connection made, you can access the JACE controller as though you were directly connected. For detailed instructions, see “[Accessing the Host or Station,](#)” page 4-43.

- Step 8** If you want to check the status of your connection or to disconnect, right-click **Dial-Up Networking Monitor** again on the taskbar.

## Windows 2000

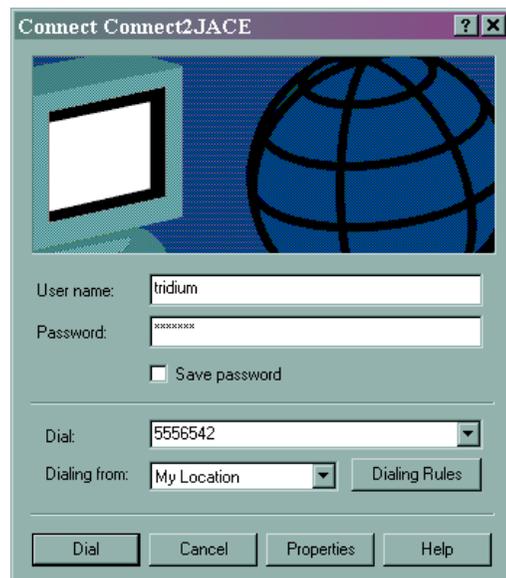
### Procedure 4-14 Making the DUN connection on Windows 2000.

- Step 1** On the Windows 2000 taskbar, select **Start > Settings > Control Panel**.
- Step 2** Double-click **Network and Dial-up Connections** then double-click the icon for the connection you want to start (this is the connection you created in [Procedure 4-12](#)).
- Step 3** Type the user name and password that provides you access to the operating system running on the remote host, and click **OK**.

**Tip**

This is the same user that you granted dial-in permissions to on the remote host.

**Figure 4-34 Supply user name and password credentials for remote host.**



RAS attempts to establish a connection between the modem on your computer and the modem on the remote host. Wait for the connection to be made.

**Step 4** If a **Connection Complete** dialog box is displayed, click **OK** to proceed.

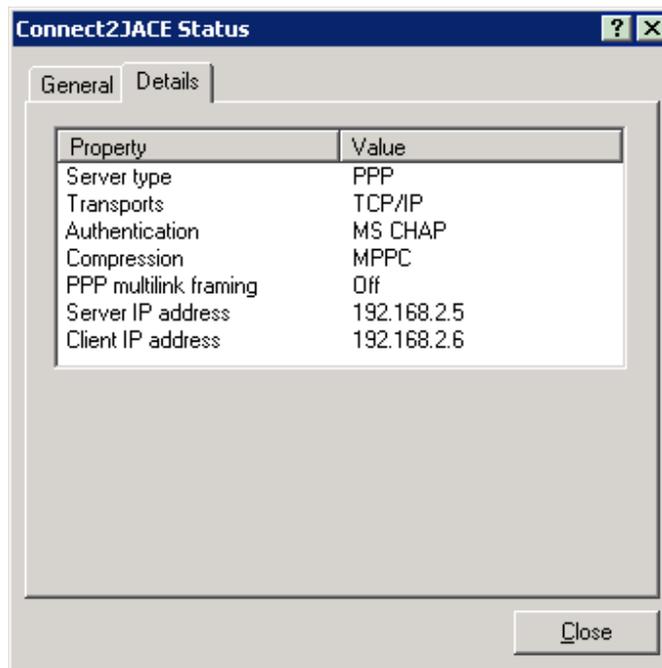
**Step 5** With the connection made, locate the **Dial-Up Networking Monitor**  on the taskbar and right-click it.

The DUN monitor is used to check the status of the connection and to discover the IP address assigned to your machine and that of the remote server.

**Step 6** Click **Status**, then click the **Details** tab (Figure 4-33).

The **Client IP Address** field displays the address assigned to your machine for this connection. The **Server IP Address** field displays the IP address of the remote server (make note of this address).

Figure 4-35 TCP/IP connection details.



With the connection made, you can access the remote host as though you were directly connected. For detailed instructions, see “[Accessing the Host or Station,](#)” page 4-43.

- Step 7** If you want to check the status of your connection or to disconnect, click the right mouse button on **Dial-Up Networking Monitor** on the taskbar.

## Accessing the Host or Station

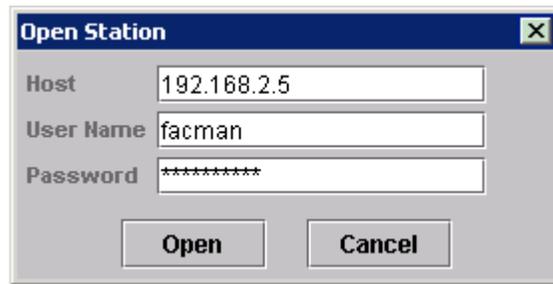
With the connection made, you launch the Niagara software, and connect to the host or station using the IP address you noted in the DUN monitor. For example, to engineer a station on the remote host, do the following:

### Procedure 4-15 Opening a station located on a remote dial-up host.

- Step 1** On the taskbar, click **Start > Programs > Niagara <release> > Java Desktop Environment**.
- Step 2** From the menu, click **File > Open Station**.  
The Open Station dialog is displayed.
- Step 3** In the **Host** text box, type the IP address of the remote host, as listed in the Dial-up Networking Monitor ([Figure 4-36](#)). If you are using Windows NT, this is the **Dial-Up Server** address; in Windows 2000 this is the **Server IP Address**.



**Tip** You can create a hosts table on your local machine, which equates this IP address to the host name of the remote host. Then you can type the host name here instead.

**Figure 4-36** Opening a station on a remote host.

**Step 4** In the **User Name** text box, type a user name to access the station.

**Step 5** In the **Password** text box, type the password.

**Step 6** Click **Open**.

The Tree View updates and displays the open (remote) station.

---

## Connecting to an ISP

---

In this chapter we discuss connecting Niagara devices to an ISP for remote access. Principal topics include:

- [Niagara Considerations](#)
- [Configuring Captive ISP on the JACE-4/5](#)
- [Configuring DDNS on the JACE-4/5](#)
- [Connecting Windows-based Hosts via Telephone Modem](#)
- [Connecting via Cable or DSL Modem](#)

This section does not cover connecting Niagara host to each other directly using modems. You can find that information in [Chapter 4, “Connecting with Direct Dial.”](#)

### Niagara Considerations

This section discusses typical system architectures and best practices when connecting Niagara devices to an ISP. It includes the following topics:

- [System Architectures](#)
- [About Connecting to an ISP](#)
- [Design Considerations](#)
- [Selecting an ISP](#)

## System Architectures

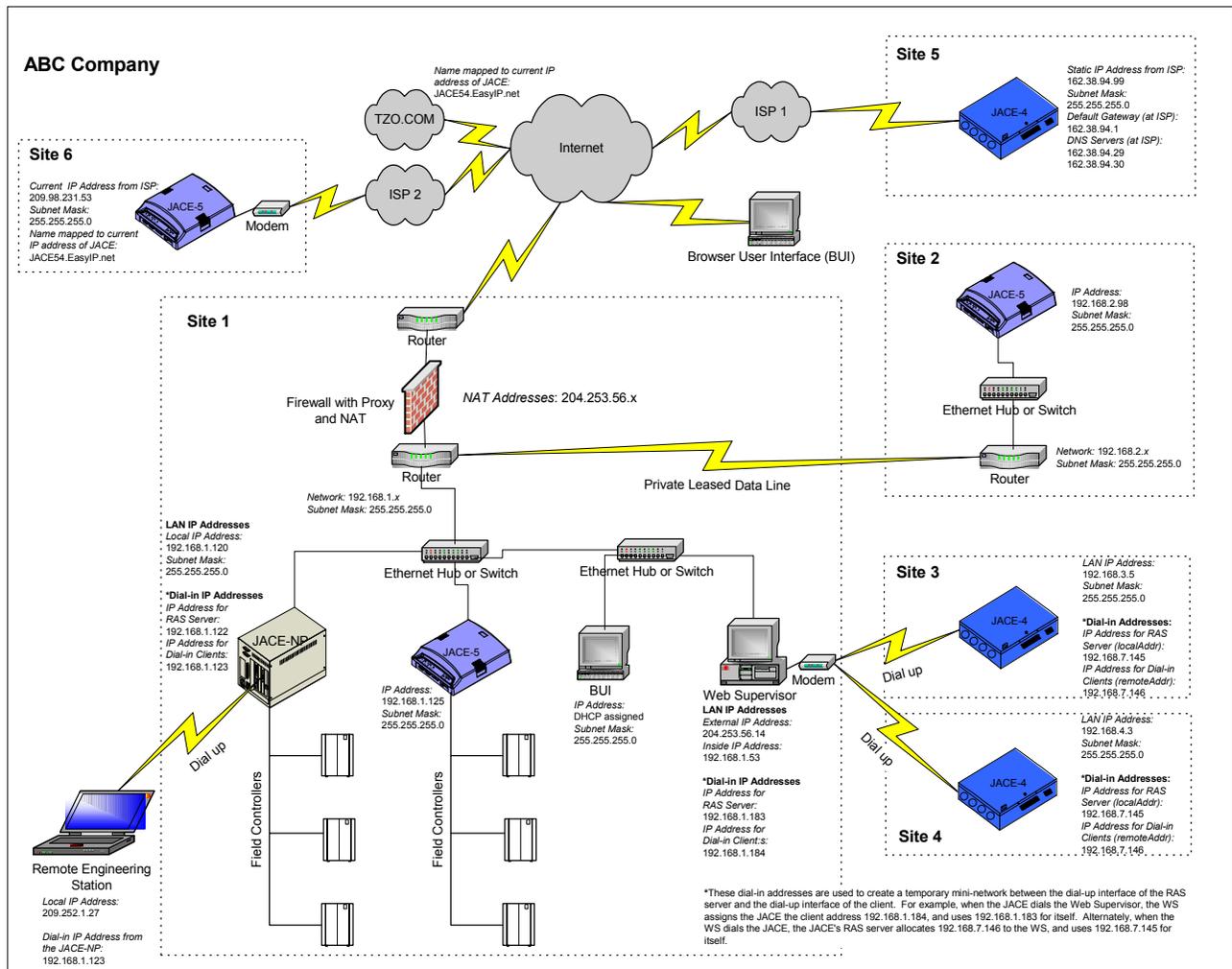
[Figure 5-1](#) provides examples of typical Niagara job configurations (system architectures) for connecting JACE-4/5s to an ISP.

In the scenario presented in [Figure 5-1](#), ABC Company has added two JACE-4/5s to remote sites (for descriptions of the other sites shown in the figure, see the “[System Architectures](#)” sections on [page 3-1](#) and [page 4-2](#)).

In site 5, the JACE has been configured to dial an ISP. Upon connection, the JACE receives a public, static IP address (and other settings for default gateway and DNS) from the ISP. It can then send archives or alarms to the Web Supervisor (since the Web Supervisor also has a public IP address). This setup also allows the Web Supervisor (or the remote engineering station, if connected to the Internet or site 1) to access the JACE using the public IP address of the JACE. The engineering stations connect to acknowledge alarms, to maintain the devices using maintenance tools such as Admin Tool, JDE, or web browser, or to pick up archives, if polled archiving is set up. When the JACE loses its connection to the ISP, it immediately redials until it is connected again. On the JACE-4/5, this configuration is known as captive ISP. For more information, see the “[About Captive ISP](#)” section on [page 5-8](#).

Site 6 also uses captive ISP, however, the JACE connects to a different ISP and this ISP does not provide a static IP address. Rather, it gives out a different public IP address each time the JACE connects to it. Therefore, the JACE at site 6 has been configured to work with a company that provides DDNS services for Internet-connected hosts (TZO.COM). Each time the JACE connects to the ISP and receives a new IP address, it sends the new address to the DDNS company, which maps the address to a fixed host name (JACE54.EasyIP.net). The JACE can still send archives or alarms to the Web Supervisor (since the Web Supervisor also has a public IP address). When the Web Supervisor (or the remote engineering station) wants to contact the JACE, it uses the host name JACE54.EasyIP.net rather than the IP address, since that may have changed since it last connected. For more information on our implementation of DDNS on the JACE-4/5, see “[Configuring DDNS on the JACE-4/5](#),” [page 5-22](#).

Figure 5-1 Typical ISP connectivity scenarios (sites 5 and 6).



## Additional Scenarios

Figure 5-2 shows some additional ISP-connectivity scenarios. Each option is discussed in the following section.



**Note**

These scenarios have not been tested by Systems Engineering. We recommend that you set up a pilot to test them before implementing in a live job.

### Connecting Windows-based Hosts via Telephone Modem

In **options 1 and 2**, two Windows-based Niagara hosts have been configured to connect to ISPs with modems. They connect using RAS and each receive public, static IP addresses (and other settings) from the ISP. However, RAS will not automatically redial on disconnect. That function must be provided by a third-party software application (such as RascalPro by Basta Computing).

If the ISP assigns dynamic IP addresses, an Internet DDNS provider (TZO or other) must provide Windows-based client software to implement DDNS on these hosts.

## Connecting Hosts via Cable or DSL

**Options 3 and 4** show connectivity to the Internet from any Niagara host via a cable or DSL modem. Note that with DSL or cable, the connection to the Niagara host is via the Ethernet connection, rather than the dial-up connection (as it is with a traditional modem). The cable or DSL provider issues a public, static IP address (and other settings) to the Niagara host.

Most cable and DSL connections are “always on”, so there may be no need to implement software that initiates connection on disconnect. If necessary (when a dynamic IP address is assigned), DDNS can be implemented on JACE-NPs or Web Supervisor, but not on a JACE-4/5, as its DDNS implementation works on the dial-up interface only.

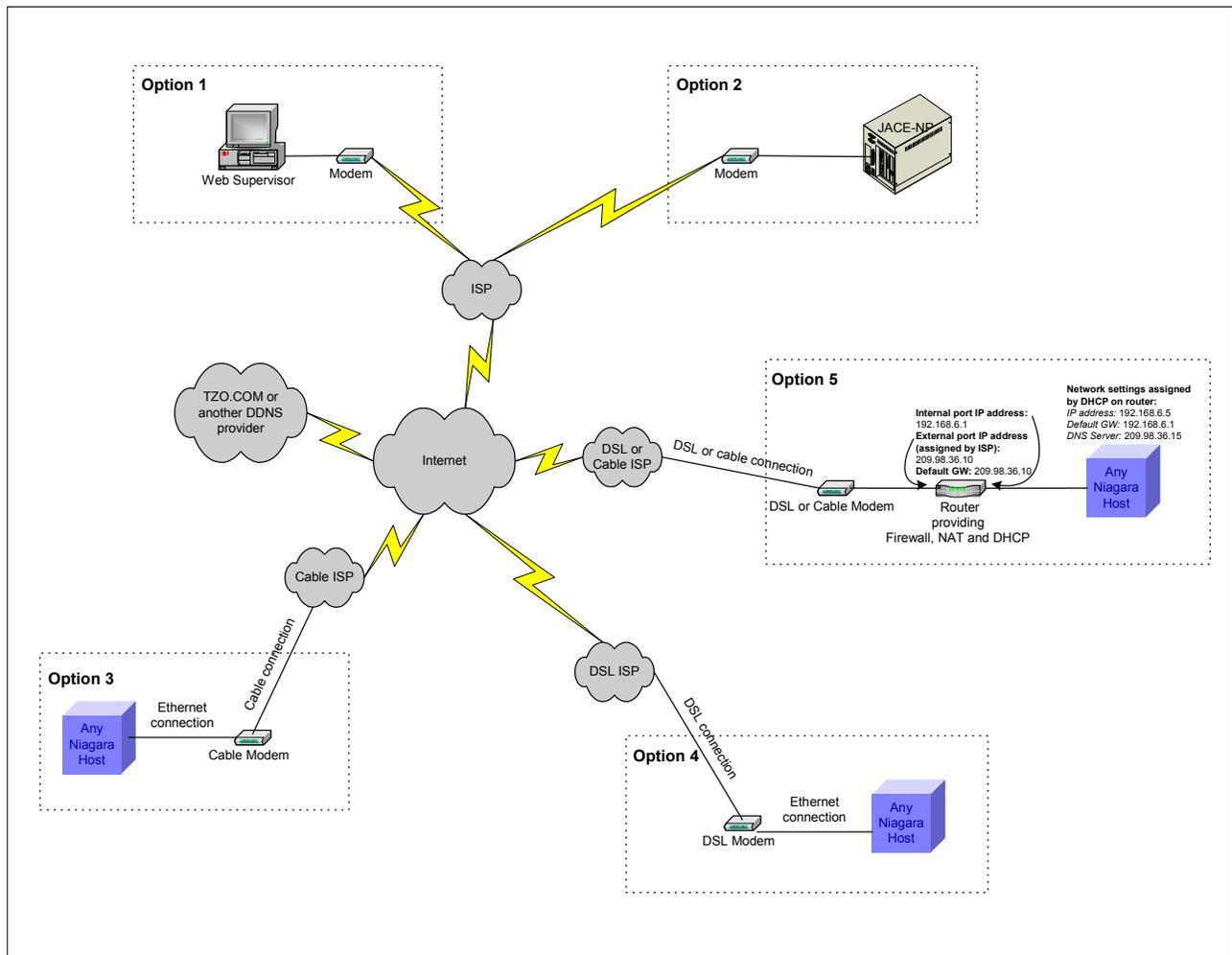
## Connections with NAT

**Option 5** shows the implementation of a NAT device in a DSL/cable scenario. The provider issues a public, static IP address (and other settings) to the account holder. That public address and other settings are used on the Ethernet port of the router connected to the DSL or cable modem. The router is configured with a private IP address on the Ethernet connection to the Niagara host, and it assigns another private IP address (and other settings) to the Niagara host. Note that the NAT function could also occur at the ISP rather than in a router located at the customer site.

This NAT scenario may not work with DDNS. In the example the Niagara host is assigned a private IP address. This is typically the address that the host reports to the DDNS provider. The host is not reachable at that private address. You would need to find some kind of software that updates the DDNS provider each time the router’s external IP address changes. That could be either:

- Client software from the DDNS provider. Note that the JACE-4/5 does not support the use of this client software in its DDNS configuration.
- Software to run on a specific model of router to handle the updating when the IP address changes on the router. These are commonly available on the Internet on sites which discuss home networking.

Figure 5-2 Other ISP connectivity scenarios.



## About Connecting to an ISP

The philosophy behind connecting a host to an ISP is different than connecting hosts with direct dial. With direct dial, the station address book is configured with information about dialing the remote host. Whenever the application needs to send data to a remote host, it uses the information in the address book to dial that host. When the data exchange finishes, the initiating host disconnects.

With an ISP connection, the ISP-connected host is assumed to be always connected. Therefore, the station does not trigger a connection when it is ready to send data—it just attempts to send it. When disconnects occur on the ISP-connected host, the host must be configured to continually retry to connect to the ISP. Data is queued in the station until the re-connection occurs. Upon successful connection data is passed between hosts.

With direct dial, there is a restriction in simultaneous user- and application-initiated data passing. If one host makes an application-initiated call, it cannot also send user-initiated data. Nor can one host make an application connection and receive user-connection data. With an ISP connected host, there is no restriction. Hosts can simultaneously pass data, of any type, just as when on a LAN/WAN.

## Design Considerations

You should note the following things about connecting Niagara hosts to an ISP:

- Connection to and from a host dialing an ISP will be slower than connection on a LAN /WAN.
- If the JACEs will be sending little data (archives and alarms) connecting (even long distance) with direct dial may be cheaper than the monthly fees for the ISP and the DDNS provider. However, dial-up has some limitations (see the [“About Dialing between Niagara Hosts”](#) section on page 4-3).
- Many IT departments prohibit setting up Internet connections on hosts attached to their network. This is considered by many departments to be a network security violation. Therefore, it is advisable to check with them before implementing the connection.
- Interstation links were designed to be used across connections that are always available. **Due to the unreliable nature of connecting to and passing data on the Internet, we do not recommend using interstation links to or from hosts connecting through an ISP.** Unlike direct dial, however, nothing prevents you from setting up the link because hosts are not identified in the station address book as dial-up hosts.

Because interstation links are not available, if you require BUI access to remote hosts you must license WebUI services on each remote JACE.

- DDNS is not supported on a JACE-4/5 when connected to an ISP via its Ethernet port (cable or DSL modem).
- TZO is the only DDNS provider supported on the JACE-4/5 platform. With other platforms you can use any DDNS provider that provides a client for the platform.
- You should plan to test functionality when connecting Windows-based hosts, or connecting any Niagara host via cable or DSL modems as these connections have not been tested by Systems Engineering.
- If NAT is used to assign a private IP address to our equipment you may not also be able to use DDNS. See the [“Additional Scenarios”](#) section on page 5-3.
- Connecting hosts to the Internet with a public IP address makes them more vulnerable to attack than connecting them via dial-up or connecting them on a private LAN/WAN. This is especially true of any host that stays connected to the Internet virtually full time (as we require of our ISP-connected hosts). For more information, see the [“Security Considerations”](#) section on page 6-1.
- There are limitations with using our equipment with a firewall. See [“Using a Firewall or Proxy Device,”](#) page 6-4.

- Many factors are involved in choosing an ISP that will work with our equipment. See [“Selecting an ISP.”](#)

## Selecting an ISP

You should think about the following things when selecting an ISP for use with our equipment:

- **Does the ISP provide a phone number that is local to the location of the equipment?** Using a local ISP saves long distance charges.
- **Does the ISP provide public IP addresses?** If not, are they using NAT or a proxy server to provide a private one? If they are using NAT, that excludes the use of DDNS, therefore they must provide a static public IP address. If they use a proxy server, you should not choose them.
- **Does the ISP provide static IP addresses or dynamic?** If the ISP provides a dynamic address you must also register with a DDNS service.
- **Does the ISP prohibit:**
  - **DDNS use?** If not, can they provide you with a permanent public IP address?
  - **clients from connecting at all times (required by our software)?**
  - **hosting a commercial application at your site?**

These items may violate the ISPs service agreement. If you cannot get them to make an exception, choose a new ISP.

- **Does the ISP block port 80 (the standard HTTP port) or other inbound ports?** If they do, then you can change the port in the application, (see the [“Changing Niagara Default Ports”](#) section on page 6-9). Changing the port is recommended for security concerns (see the [“Selecting an ISP”](#) section on page 5-7). Another approach is for you to purchase an HTTP port forwarding service, which maps a call to the standard HTTP port to another port of your choosing (TZO.com offers this).
- **Does the ISP provide:**
  - **firewall services?** You could have them set up access restrictions for you.
  - **domain name registration services?** Typically you would do this only if the customer requires it. Domains registered through an ISP are typically tied to equipment serviced by that ISP.

Some DDNS service providers also provide a domain registration service that would allow you to have one domain name for hosts that are serviced by multiple ISPs.
  - **one e-mail address with the account?** If you are going to set up e-mail notification on the Niagara host, then you must have either:
    - a valid mail account with the ISP
    - know of an Internet mail server that relays mail (most do not).

For more information on setting up the mail service and e-mail notifications, see the *Niagara Standard Programming Reference*.

# Configuring Captive ISP on the JACE-4/5

In order to connect your JACE-4/5 to an ISP, you must configure the captive ISP service. The following topics guide you through configuring captive ISP:

- [About Captive ISP](#)
- [Installing and Configuring Modems](#)
- [Configuring the Software](#)
- [Troubleshooting Connection Problems](#)

## About Captive ISP

When configured to use the captive ISP service, the Niagara software `daemon` dials the ISP when the JACE-4/5 boots. If the JACE ever loses the connection, it immediately tries to reconnect, whether or not it has any data to send to another host. Once the JACE establishes connection to the ISP, all access to the JACE is through the IP address assigned by the ISP.

Captive ISP is unlike direct-dial mode, where the station dials a specially-configured host only when it has data to send to it; rather the station assumes that the JACE is always connected. Also unlike direct dial, multiple stations and GUI tools (e.g., browser, Admin Tool, JDE) can access the JACE simultaneously through the IP address assigned by the ISP. In addition, address book entries for other hosts are configured using the IP address or host name rather than the dial-up properties.

## About Disconnects

If the JACE cannot connect to the ISP after a configurable number of attempts, the JACE will listen for a period of time (also configurable) for incoming calls. The JACE will periodically attempt to reconnect to the ISP. This is one window where the modem is free and you can successfully dial into the JACE. For more information, see the `ispRetryCount` and `ispRetryDelay` parameters in “[Configuring ras.properties for Captive ISP](#),” page 5-10.

In addition to this unscheduled type of disconnect, we supply two additional methods of controlled disconnects.

### Release 2.2 and earlier

The JACE-4/5 can also be configured to disconnect from the ISP up to 6 times per day for a configurable number of minutes. While the JACE-5 is disconnected, it will listen for incoming calls on the modem. When the disconnect duration expires, the JACE will automatically redial the ISP. For more information, see the `ispDisconnectn` parameters, explained in “[Configuring ras.properties for Captive ISP](#),” page 5-10.

### Release 2.3 and later

The JACE-4/5 can be configured to disconnect from the ISP by using a Niagara object tied to a Schedule object that you configure. For more information, see “[Using the IspConnection Object to Control Disconnects](#),” page 5-15.

## Installing and Configuring Modems

Just as with a direct dial connection, configuration of the JACE-4/5 begins with modem configuration. If you are unfamiliar with installing and configuring modems on JACE-4/5s, refer to the “[Installing and Configuring Modems](#)” section on page 4-7. Step-by-step instructions for configuring modems are also included in “[Configuring ras.properties for Captive ISP](#),” page 5-10.

## Configuring the Software

Configuring our software for captive ISP is a multi-step process. Use the following topics to guide you through the process:

- [Information Required from the ISP](#)
- [Configuring Network Settings for Captive ISP](#)
- [Configuring ras.properties for Captive ISP](#)
- [Granting Dial-in Permissions](#)
- [Using the IspConnection Object to Control Disconnects](#)
- [E-mail Configuration](#)

### Information Required from the ISP

You will need the following information from the ISP:

- user name and password
- telephone access numbers
- host and domain name of the JACE
- IP address of one or more DNS servers
- outgoing (SMTP) mail server name and e-mail address (if configuring e-mail notification)
- Network settings assigned by the ISP to include:
  - IP address (if static)
  - subnet mask

### Configuring Network Settings for Captive ISP

To begin you must configure some (but not all) of the network settings of the JACE. Normally, these settings apply to the Ethernet interface of the JACE, but captive ISP uses some of them for the dial-up interface.

#### Procedure 5-1 Configuring network settings for captive ISP.

---

- Step 1** Using the **Admin Tool**, connect to and log into the JACE.
- Step 2** Click the **Network Settings** tab.
- Step 3** Fill in the following information from the information provided to you by the ISP:
- **DNS Domain**
  - **Subnet Mask**
  - **DNS Servers**



**Note** Do not change the information in the **IP Address** text box. This is the IP address of the LAN interface (if used). You set the IP address of the dial-up interface in the `localAddr` parameter of the `ras.properties` file.

**Step 4** Remove any information in the **Default Gateway** text box to leave it blank.



**Note** The default gateway function will be handled by the routers at the ISP. If you leave this set to the default gateway on the LAN, packets intended for the ISP (and the Internet) will be routed to the Ethernet interface (and onto the LAN, if one is attached).

**Step 5** Click **Apply**.



**Caution** Do **not** reboot at this time. Rebooting prematurely could render the JACE unreachable via the LAN. Reboot only when finished implementing the remainder of the RAS settings. If you do reboot prematurely and lose contact with the JACE, see “[Troubleshooting Connectivity to an Existing JACE Controller](#),” page 3-14 to find out how to reestablish connection.

## Configuring ras.properties for Captive ISP

The `ras.properties` file is used to configure both direct dial and captive ISP (and the modem). In [Table 4-1](#) we examined the properties of this file that applied to direct dial (see also “[About the ras.properties File](#),” page 4-12). In [Table 5-1](#) we examine the ones that apply to captive ISP.

**Table 5-1** Parameters of the `ras.properties` file used to configure captive ISP.

| Section            | Parameter   | Valid Values and Default Values (in Bold) | Description                                                                                                                                                                                                   |
|--------------------|-------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties | rasEnable   | true<br><b>false</b>                      | Change this to true to enable RAS for this JACE-4/5. The modem will not accept calls when this setting is false. In addition, when this is false, the JACE will not attempt to initialize any attached modem. |
|                    | rasMode     | <b>directDial</b><br>captiveISP           | Use captiveISP for this function. Direct dial mode is discussed in <a href="#">Chapter 4, “Connecting with Direct Dial.”</a>                                                                                  |
|                    | dialOutOnly | true<br><b>false</b>                      | Set this to true and the JACE will not accept incoming calls. For captive ISP, you should leave this at false so that you can dial into the JACE should it ever disconnect from the ISP.                      |

Table 5-1 Parameters of the ras.properties file used to configure captive ISP. (continued)

| Section                        | Parameter       | Valid Values and Default Values (in Bold)                                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties             | remoteAddr      | any valid IPv4 address in dotted decimal notation<br><b>192.168.1.111</b>                                                                               | The IP address of the remote machine you are dialing into. For most ISPs you do not need to specify this parameter. You should remove the default value (remoteAddr= ) or comment out the line (#remoteAddr=192.168.1.111) so the JACE accepts whatever address the ISP assigns.                                                                                                                                                                                                                                                                                                                                                                                                |
|                                | localAddr       | any valid IPv4 address in dotted decimal notation<br><b>disabled</b>                                                                                    | Specifies the IP address of the dial-in interface on the JACE. If the ISP requires the JACE to request a specific static IP address, you must specify it using this parameter. When this parameter is absent (or left blank), the JACE accepts whatever dynamic IP address is assigned by the ISP.<br><b>Release 2.2 and earlier</b> —If you specify an address for this parameter that does not match what the ISP assigns to the JACE, the JACE will not connect to the ISP.<br><b>Release 2.3</b> —If you specify an address for this parameter that does not match what the ISP assigns to the JACE, the JACE will ignore your setting and use the address the ISP assigns. |
| Modem Configuration Properties | device          | COM1<br><b>COM2</b>                                                                                                                                     | The COM port used by the modem. If using the JACE-4 internal modem, this should remain at COM2. If using an external modem with the JACE-4, this should match the serial port assignment of the RS-232 port as listed in the port.properties file (see <a href="#">“Enabling the JACE-4 Modem (Internal or External),”</a> page 4-10).                                                                                                                                                                                                                                                                                                                                          |
|                                | baudrate        | <b>57600</b><br>48800<br>36600<br>19200                                                                                                                 | The initial baud rate to use between the JACE and the modem. In most cases you will not have to change this parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                | initString      | depends on modem<br>• <b>JACE-5—AT&amp;F1E0X4</b> (USR Sportster)<br>• <b>JACE-4—ATE0Q0V1X4&amp;D2&amp;K3\N3%C2&amp;C1&amp;Q5W2</b> (internal Cermetek) | The modem-specific initialization string sent to the modem when the JACE boots. It sets options required by our hardware (see the <a href="#">“About Pre-configured Modems”</a> section on page 4-7).<br>Initialization string for the Zoom External V.90 Dualmode Faxmodem— AT&FE0S0=0                                                                                                                                                                                                                                                                                                                                                                                         |
|                                | updateNvRamCmd  | depends on modem<br><b>AT&amp;W0</b> (USR Sportster)                                                                                                    | Modem specific command used to save the initialization string to <b>O</b> so it is available to initialize the modem if the modem reboots and the JACE does not.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                | updateNvRamFlag | <b>false</b><br>true                                                                                                                                    | Set to true to save the initialization string to NVRAM during the next boot. This flag must be manually set to true each time <a href="#">initString</a> is changed. The JACE will automatically set this back to false after the NVRAM has been successfully updated. This prevents unnecessary writes to modem NVRAM.                                                                                                                                                                                                                                                                                                                                                         |
|                                | initFailLogOnly | <b>false</b><br>true<br><b>Note:</b> Supported in release 2.3 or later.                                                                                 | When set to false, the JACE will reboot up to three times in order to initialize the modem if it does not respond on the first boot. If the modem is not initialized by the third time, a message is sent to the Admin Tool’s event log. When set to true, the JACE will not reboot if the modem doesn’t initialize, but will only send a message to the event log.                                                                                                                                                                                                                                                                                                             |

Table 5-1 Parameters of the ras.properties file used to configure captive ISP. (continued)

| Section                                                                                                      | Parameter                                                                                                                        | Valid Values and Default Values (in Bold)                                                                                                                                                                                                                                                                                                                                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISP Configuration Properties                                                                                 | ispPrimaryNumber                                                                                                                 | any valid phone number, including any numbers used to access an outside line and any number of pause characters (.)<br><b>9,5551234</b>                                                                                                                                                                                                                                                                                                                          | The primary phone number that the JACE dials to reach the ISP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                              | ispBackupNumber                                                                                                                  | any valid phone number, including any numbers used to access an outside line and any number of pause characters (.)<br><b>9,5551234</b>                                                                                                                                                                                                                                                                                                                          | A secondary phone number that the JACE can dial to reach the ISP. If the JACE fails to connect on the primary number, the secondary number is used until it fails to connect, then the primary one is used.<br><br>If the ISP only has a single access number, change this value to the same value as the ispPrimary number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                                                                                              | ispUsername                                                                                                                      | any combination of letters, numbers and special characters<br><b>user@isp</b>                                                                                                                                                                                                                                                                                                                                                                                    | The user name given to you by the ISP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                                                                              | ispPassword                                                                                                                      | any valid password<br><b>password</b>                                                                                                                                                                                                                                                                                                                                                                                                                            | The password of the user name given to you by the ISP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                                                                              | ispRetryCount                                                                                                                    | any integer<br><b>1</b>                                                                                                                                                                                                                                                                                                                                                                                                                                          | When the JACE fails to connect to the ISP, it reverts to dial-in mode, where it waits for an incoming call. The retry count specifies the number of failed dial attempts that occur before the JACE switches to dial-in mode. Used in tandem with the <a href="#">ispRetryDelay</a> parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                              | ispRetryDelay                                                                                                                    | any integer<br><b>2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                          | The retry delay specifies the number of minutes that the JACE listens for incoming calls before attempting to dial another connection. Used in tandem with the <a href="#">ispRetryCount</a> parameter.<br><br>For example, if the retry count is 3 and the retry delay is 10, the JACE will dial the ISP 3 times (alternating between primary and backup number) in succession. If all 3 attempts fail, it will then revert to dial-in mode for 10 minutes before making another 3 connection attempts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                                              | ispDisconnectTime1<br>ispDisconnectTime2<br>ispDisconnectTime3<br>ispDisconnectTime4<br>ispDisconnectTime5<br>ispDisconnectTime6 | A set of integers in the form <i>hh:mm-n</i> where <ul style="list-style-type: none"> <li><i>hh</i> is time in a 24-hour format (0-23)</li> <li><i>mm</i> is the minutes past the hour (0-59)</li> <li><i>n</i> is the disconnect duration in minutes</li> </ul> For example:<br>ispDisconnectTime1=8:35-5 (disconnect at 8:35 a.m. and stay disconnected for 5 minutes)<br>ispDisconnectTime2=0:00-60 (disconnect at midnight and stay disconnected for 1 hour) | These parameters allow you to set up regulated disconnect times for the modem. You can schedule up to 6 disconnects (with a configurable duration) in a 24-hour period. When the disconnect duration expires, the JACE automatically redials the ISP. You must use a unique <code>ispDisconnectTime<i>n</i></code> for each disconnect you want to schedule.<br><br>A disconnect session may not cross midnight. If the JACE must stay disconnected from 11:00 p.m. 1:00 a.m., you must make 2 entries, one from 11:00 pm to midnight (23:00-60) and another from midnight to 1 am (0:00-60).<br><br>The Niagara station maintains the time of day clock for this feature. The station handles adjustments to GMT for daylight saving times and time zone. Therefore, if the station is not running, the disconnect feature is disabled.<br><br><b>Note:</b> If any entry contains any invalid values, it is ignored.<br><br>For release 2.3 or later, you schedule disconnects using a Niagara object. See <a href="#">"Using the IspConnection Object to Control Disconnects,"</a> page 5-15. |
| <b>Note:</b> These parameters are not listed in the ras.properties file but you can add them when necessary. |                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Table 5-1 Parameters of the ras.properties file used to configure captive ISP. (continued)

| Section                  | Parameter  | Valid Values and Default Values (in Bold) | Description                                                                                                                                                                                                                                                   |
|--------------------------|------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Miscellaneous Properties | pppDebug   | <b>false</b><br>true                      | Set to true to see dial-up troubleshooting information. This information is written to the VxWorks target shell and is accessible via direct connect (Hyperterminal) or over a LAN connection (Telnet). See "Troubleshooting Connection Problems," page 5-19. |
|                          | modemDebug | <b>false</b>                              | Set to true to see dial-up troubleshooting information. This information is written to the VxWorks target shell and is accessible via direct connect (Hyperterminal) or over a LAN connection (Telnet). See "Troubleshooting Connection Problems," page 5-19. |
|                          | rasDebug   | true                                      |                                                                                                                                                                                                                                                               |
|                          |            |                                           | <b>Note:</b> Neither of these parameters is listed in the ras.properties file but you can add them.                                                                                                                                                           |

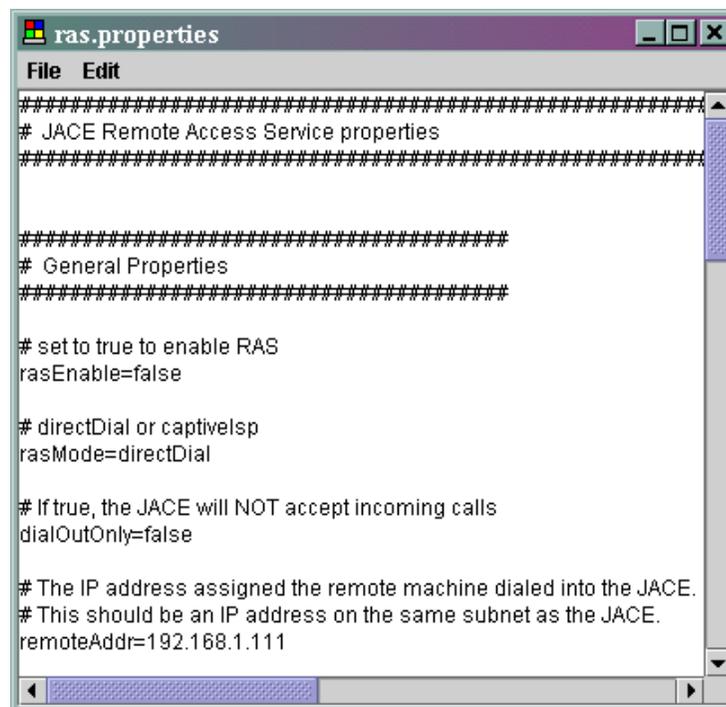
Use the following steps to configure the JACE-4/5 for captive ISP.

**Procedure 5-2 Configuring the JACE-4/5 for direct dialing.**

- Step 1** Using the **Admin Tool**, connect to and log into the JACE.
- Step 2** Click the **Network Settings** tab.
- Step 3** Click **Edit Modem Properties**.

The ras.properties file is opened for editing (Figure 5-3).

**Figure 5-3** ras.properties file opened for editing.





**Note** The first time you view the `ras.properties` file, it contains remarks explaining each setting. The remark lines are preceded by a pound sign (see the example above). After saving the file, the remarks are stripped out and any future edits of the file will not contain the remarks.

**Step 4** Edit the file using the information in [Table 5-1](#) as a guide. At a minimum, you must configure the following items:

#### General Properties

- `rasEnable`—change **false** to **true**
- `rasMode`—change **directDial** to **captiveISP**.
- `dialOutOnly`—leave this at **false** to allow dial-in to the JACE upon disconnect. Otherwise, change this to **true**.
- `remoteAddr`—set this as described in the **Description** column of [Table 5-1](#).
- `localAddr`—set this as described in the **Description** column of [Table 5-1](#). If the parameter is missing, add it in the form `localAddr=<value>`.

#### Modem Configuration Properties

- `device`—change to **COM1** if your modem is attached to that port.
- `initString`—change if you are using a modem other than those that we have pre-configured.



**Tip** The Sportster and Zoom initialization strings and update NVRAM commands are pretty standard. Consider trying them with your modem to see if they work for you.

- `updateNvRamCmd`—change if you are using a modem other than those that we have pre-configured.
- `updateNvRamFlag`—change **false** to **true** if you have updated the initialization string.

#### ISP Configuration Properties

- `ispPrimaryNumber`—set this as described in the **Description** column of [Table 5-1](#).
- `ispBackupNumber`—set this as described in the **Description** column of [Table 5-1](#).
- `ispUsername`—set this as described in the **Description** column of [Table 5-1](#).
- `ispPassword`—set this as described in the **Description** column of [Table 5-1](#).
- `ispRetryCount`—set this as described in the **Description** column of [Table 5-1](#).
- `ispRetryDelay`—change this as described in the **Description** column of [Table 5-1](#). Be sure to set the time associated with this parameter considerably longer than the time referenced in `ispRetryCount`.

**Step 5** If you want to set up a disconnect schedule, add one or more of the following parameters in the ISP Configuration section, as described in the **Description** column of [Table 5-1](#):

- `ispDisconnectTime1`
- `ispDisconnectTime2`
- `ispDisconnectTime3`
- `ispDisconnectTime4`
- `ispDisconnectTime5`
- `ispDisconnectTime6`



**Note** You must use a unique `ispDisconnectTimen` for each disconnect you want to schedule.

**Step 6** From the file menu, choose **File > Close**.

If you made any changes, you are prompted to save them, otherwise the window closes.

**Step 7** If prompted to save your changes, click one of the following:

- **Yes** to save your changes. The file saves and the window closes.
- **No** to discard your changes. The window closes.
- **Cancel** to return to the editing window, then refer to [Step 4](#).

**Step 8** Reboot the JACE.

## Granting Dial-in Permissions

If any host is going to connect to RAS on the JACE controller you must grant the connecting user dial-in permissions. You do this on the Users tab of the Admin tool. For complete instructions, refer to the [“Enabling Dial-in”](#) section on page 4-16.

## Using the IspConnection Object to Control Disconnects

A new module (`isp`) and object (`IspConnection`) have been added to the `tridiumx` folder in release 2.3. They allow you to control the disconnect schedule of a JACE-4/5 within the station. These replace the disconnect schedule in `ras.properties` used in previous releases.

Using the module and object gives you the following advantages:

- **Standard schedule object can be used to control the disconnect schedule**—This provides greater flexibility (and familiarity) in scheduling connects and disconnects.
- **GxPage access to the schedule**—GUI access to the schedule is more convenient for your clients.
- **Enhanced logging and notification of connection problems**—The station can log and report connection problems via the alarm console of a Web Supervisor or a notification recipient.
- **Disconnect overrides**—Provides a method to force a connection when a critical point alarms.

**Notes**

- With the `IspConnection` object, the connect/disconnect schedule resides in the station rather than being managed by the Niagara `daemon`. Therefore, if the station on the JACE is not running, the JACE will not follow the disconnect schedule. For more information, see the “[Troubleshooting Connection Problems](#)” section on page 5-19.
- The `IspConnection` object can only be used with the captive ISP function, not with the direct dial function.

The object has one input (`sIn` or `statusIn`). To establish a connection, use a schedule or other binary object to set `sIn` to Active. To terminate the connection, set `sIn` to Inactive. When inactive, the modem will resort to either idle, or listening as configured in the `dialOutOnly` parameter in `ras.properties`.

**Note**

The object passes your connection request to the Niagara `daemon`, which implements it on its next cycle. There can be a delay from when the command is issued and the daemon begins the connection process.

The object also has several output status properties, as listed in [Figure 5-2](#).

**Table 5-2 Outputs of the `ispConnection` object.**

| Output                                | Valid Values                                                                                                                                                                                                                                                                            | Description                                                               |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <code>statusOutput</code>             | Active<br>Inactive                                                                                                                                                                                                                                                                      | Indicates if there is a currently active connection.                      |
| <code>state</code>                    | <ul style="list-style-type: none"> <li>• IDLE (<code>dialOutOnly</code> parameter set to true)</li> <li>• DIALING</li> <li>• LISTENING (<code>dialOutOnly</code> parameter set to false)</li> <li>• HANGING_UP</li> <li>• CONNECTED_AS_CLIENT</li> <li>• CONNECTED_AS_SERVER</li> </ul> | Represents the current state of the modem.                                |
| <code>rate</code>                     | various                                                                                                                                                                                                                                                                                 | The connected baud rate as reported in the connect string from the modem. |
| <code>lastSuccessfulConnection</code> | any time, date, and time zone in the form:<br>hh:mm dd-mmm-yy ZZZ                                                                                                                                                                                                                       | The start time, day, and time zone of the last successful connection.     |
| <code>lastConnectionAttempt</code>    | any time, date, and time zone in the form:<br>hh:mm dd-mmm-yy ZZZ                                                                                                                                                                                                                       | The start time, day, and time zone of the last connection attempt.        |

**Examples**

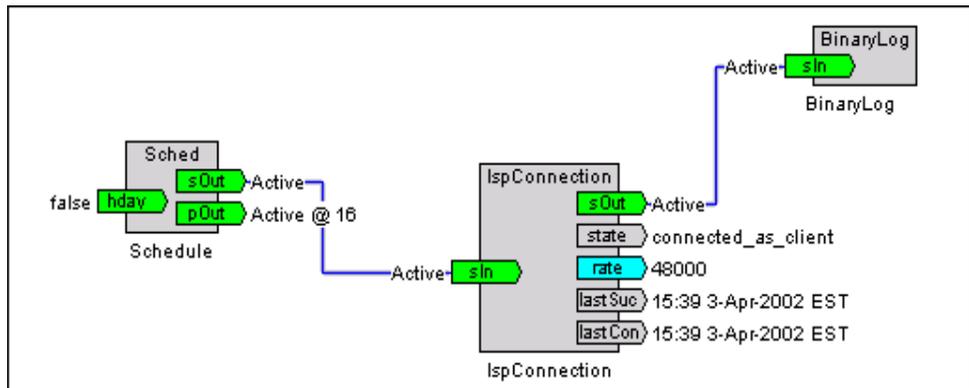
You can connect the `statusOutput` to boolean or `GxText` objects, and the `state`, `rate`, and connection outputs to text objects.

[Figure 5-4](#) shows examples of an `ISPConnection` object in use. [Figure 5-5](#) shows a simple `GxPage` containing information from the outputs of the `IspConnection` object.

**Figure 5-4** Typical IspConnection object logic.

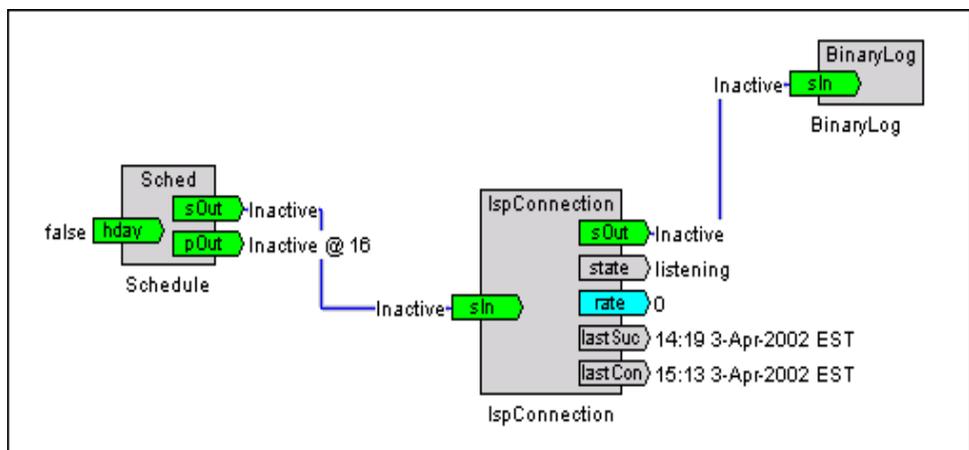
In the example at the right, a schedule object controls the connect/disconnect schedule of the IspConnection object. A binary log object logs each change of state (from active to inactive).

The JACE successfully connected to the ISP as a client, with a baud rate of 48 K.

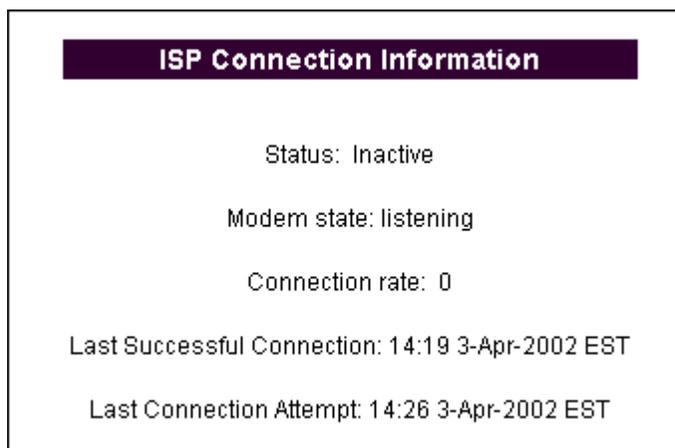


This example shows that the modem successfully connected to the ISP at 14:19 on 3-April. However line problems forced a hang up. Since the schedule showed "Active", the daemon tried to reconnect until an "Inactive" status was received at 15:15 when the active schedule expired. The daemon made its last connection attempt at 15:13 on 3-April.

The current state of the modem is listening, because the dialOutOnly parameter of the ras.properties file is set to false.

**Figure 5-5** GxPage use of IspConnection object outputs.

This simple GxPage illustrates the use of GxText objects linked to each output of the IspConnection object.



For more information about programming objects, see the *Niagara Standard Programming Reference*.

## Installing and Configuring the Module

Use the following steps to install and configure the module and object:

---

### Procedure 5-3 Installing and configuring the isp module and the ispConnection object.

---

- Step 1** Install release 2.3 on your engineering workstation and the JACE.
- Step 2** Configure and test captive ISP and DDNS (if required). Proceed only when working correctly.
- Step 3** Install the **isp** module, as follows:
- a. From your engineering workstation, connect to and log into the JACE.
  - b. Click the **Installation** tab.
  - c. Click **Installation Wizard**. You see the **Select Distribution Directory** dialog box.
  - d. Browse to the location of the distribution installation files and click the **emb** folder. You may have copied these files to your hard drive, or you can find them on the Web Supervisor installation CD.
  - e. Click **Install**.
  - f. On the **Niagara Remote Installation** window, click **Configure Modules Only** and click **Next**. The **Configure Modules** dialog box opens.
  - g. Scroll down the list of modules to install and click in the **Upgrade/Add** column of the **isp** module. The module is marked for addition with a check mark.
  - h. Click **Next**.
  - i. Choose to backup the database by supplying the administrator name and password, and click **Next**. The Niagara license window opens.
  - j. Click **Finish**.
- Step 4** Copy the **ispConnection** object from the local library to the station, as follows:
- a. In the tree view of the JDE, open the local library.
  - b. In the local library, locate the **ispConnection** object in the **tridiumx\isp\objects** directory.
  - c. Copy the object and paste it into the root or into a container on the JACE.




---

**Tip** If the JACE reboots and the object is not on the JACE, verify that the **isp** module is installed.

---

- Step 5** Configure the **ispConnection** object as described previously and test functionality.
-

## E-mail Configuration

If you are using the notification service to send e-mail notifications, you must install, then configure the mail service with the following information provided to you by the ISP:

- **SMTP server**—host name or IP address of the simple mail transfer protocol (SMTP) server. On the Config tab of the mail service, enter this in the **smtpHost** text box.
- **E-mail address**—the e-mail address the ISP has assigned to the mailbox (typically in the form `username@domain.com`). On the Config tab of the mail service, enter this in the **fromAddress** text box.
- **User name**—the user name for the mail account. Typically this will be the username portion of the e-mail address. On the Config tab of the mail service, enter this in the **username** text box.
- **Password**—the password for the mail account. On the Config tab of the mail service, enter this in the **password** text box.

For more information on setting up the mail service and e-mail notifications, see the *Niagara Standard Programming Reference*.

## Troubleshooting Connection Problems

The Niagara **daemon** (not the Niagara station) initiates and manages all ISP connections. The daemon must handle the dial-up duties because it is sometimes desirable for the JACE-4/5 to connect to the ISP while the station is not running (during a software upgrade, for example).

Since the connection is managed by the daemon and not the Niagara station, diagnostic output will not appear in the standard output window of the station (accessible via Admin Tool). However, the JACE-4/5 does log ISP connect and disconnect events in the event log. This log is accessible using the Admin Tool (**Host** > **View Event Log**) or a browser at `http://<host_name_or_ip_address>:3011/system/eventLog`.



### Notes

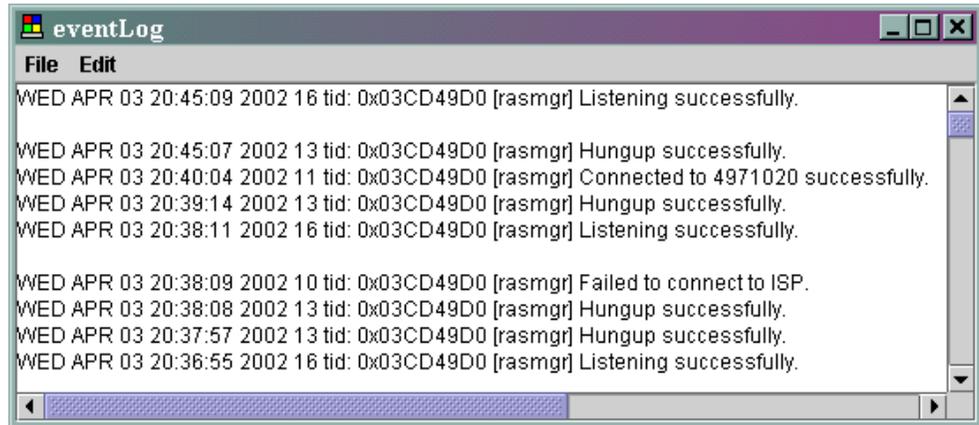
- The event log is only available on JACE-4/5s.
- If accessing the event log with a browser, be sure to capitalize “eventLog” as shown in URL.

The daemon logs the following dial-up events in the event log:

- Connects (including the IP address assigned to the JACE)
- Disconnects
- Connect failures (after the retry count is exhausted)

**Figure 5-6** provides an example of ISP connects and disconnects written to the event log.

Figure 5-6 Event log ISP connect and disconnect events.



Troubleshooting information is also written to the VxWorks target shell, which is accessible via direct connect with [Hyperterminal](#) or over an IP connection with [Telnet](#) (see “[Niagara Configuration Tools,](#)” page 2-1). You can see additional troubleshooting information by enabling the debug parameters listed in [Table 5-1](#). If you cannot connect to the JACE over the Internet, you must use one of these alternate forms of connection to view error information.

[Example 5-1](#) shows connection troubleshooting information written to the target shell **without** the debug parameters turned on. The problem diagnosed in this example is a lack of a dial tone on the line the modem is using to dial the ISP.

Example 5-1 Typical connection troubleshooting information as written to the VxWorks target shell.

| Troubleshooting Information                                     | Description                                                                                                  |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| -> [rasmgr] Handler loop pass.                                  | RAS manager sees an ISP connect request during its execution cycle and prepares the modem to dial.           |
| [dialup] Trying an isp connect.                                 |                                                                                                              |
| [rasmgr] Handler loop pass.                                     |                                                                                                              |
| [rasmgr] Attempting to hangup.                                  |                                                                                                              |
| [modem:COM2 ] Received hangup request.                          |                                                                                                              |
| [modem:COM2 ] Received wakeup message.                          |                                                                                                              |
| [modem:COM2 ] Error waiting for read in listen                  |                                                                                                              |
| [modem:COM2 ] Received error trying to process 1 msg.           |                                                                                                              |
| [modem:COM2 ] Detected dropped CD in hangup.                    |                                                                                                              |
| [modem:COM2 ] Sleeping 0 seconds to make sure line is clear.    |                                                                                                              |
| [modem:COM2 ] Modem should now be clear.                        |                                                                                                              |
| [modem:COM2 ] Waiting for message notification in OUTER loop.   |                                                                                                              |
| [modem:COM2 ] Entering modem handler INNER loop with 3 message. |                                                                                                              |
| [modem:COM2 ] Waiting for message notification in OUTER loop.   |                                                                                                              |
| [rasmgr] Hungup successfully.                                   | RAS manager sends a message to dial the phone number of the ISP, which is listed in the ras.properties file. |
| [rasmgr] Attempting to connect to <4971020>.                    |                                                                                                              |
| [modem:COM2 ] Received dial request.                            |                                                                                                              |
| [modem:COM2 ] Entering modem handler INNER loop with 2 message. |                                                                                                              |
| [modem:COM2 ] Setting modem to dial 4971020.                    |                                                                                                              |

**Example 5-1** Typical connection troubleshooting information as written to the VxWorks target shell.

| Troubleshooting Information                                           | Description                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [modem:COM2 ] Initializing modem with ATE0Q0V1X4&D2&K3\N3%C2&C1&Q5W2. | Modem is initialized, and dials the ISP. Receives a <b>NO DIALTONE</b> error.                                                                                                                                                                                   |
| [modem:COM2 ] Wrote 31 bytes to modem.                                |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Received OK on init.                                    |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Dialing <ATDT4971020>.                                  |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Wrote 12 bytes to modem.                                |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Dial response was <NO DIALTONE>.                        |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Received error trying to process 2 msg.                 |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Detected dropped CD in hangup.                          |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Sleeping 5 seconds to make sure line is clear.          |                                                                                                                                                                                                                                                                 |
| [rasmgr] Unable to achieve CONNECTED_AS_CLIENT_STATE to connect.      | RAS manager sees the error and starts the hangup process.                                                                                                                                                                                                       |
| [rasmgr] Attempting to hangup.                                        |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Received hangup request.                                |                                                                                                                                                                                                                                                                 |
| <additional lines removed>                                            |                                                                                                                                                                                                                                                                 |
| [rasmgr] Hungup successfully.                                         | RAS manager initiates the listen process (as defined by the <a href="#">dialOutOnly</a> property of the ras.properties file).                                                                                                                                   |
| [rasmgr] Attempting to listen.                                        |                                                                                                                                                                                                                                                                 |
| [modem:COM2 ] Received listen request.                                |                                                                                                                                                                                                                                                                 |
| <additional lines removed>                                            |                                                                                                                                                                                                                                                                 |
| [rasmgr] Listening successfully.                                      | Execution cycle begins again. If the ISP connection schedule indicates that a connection is required, the RAS manager starts the connection process again. Otherwise, the normal execution cycle continues until the RAS manager receives a connection request. |
| [rasmgr] Handler loop pass.                                           |                                                                                                                                                                                                                                                                 |

You can also receive limited troubleshooting information when using the `ispConnection` object. See the [“Using the IspConnection Object to Control Disconnects”](#) section on page 5-15.

## Avoiding Automatic Disconnects

Some ISPs disconnect a host when it has not sent or received packets for a period of time. If your JACE is subject to this automatic disconnect you can configure the JACE to periodically update its time. Add the TimeSync service to the station and configure it so the JACE requests a time update more frequently than the ISP’s disconnect period of time.

For more information on configuring the time synchronization service, see the *Niagara Standard Programming reference*. See also [“Changing the Time Synchronization Port,”](#) page 6-17.

## Configuring DDNS on the JACE-4/5

The dynamic domain name service (DDNS) allows a device with a dynamic IP address to be accessed using a well-known domain name. DNS servers handle mapping a name (such as JACE54.EasyIP.net) to an IP address. With DDNS, each time a host receives a new IP address, it sends an update to the name-to-IP-address mapping on the DDNS server. The DDNS function can be implemented on hosts connecting to an internal LAN (with company DDNS servers) and the Internet (with third-party DDNS services).

When configuring a JACE with captive ISP, many times you cannot obtain a static IP address for the JACE from the ISP. The random IP address makes accessing the JACE-5 via a browser or GUI tool very difficult. To overcome this limitation a DDNS client has been implemented on the JACE-4/5. The DDNS implementation on the JACE-4/5 works with one Internet DDNS provider, the Tzolkin Corporation (TZO).

### About TZO

To implement DDNS, you must purchase an annual DDNS subscription from TZO for each JACE. TZO provides you a software key, which is the unique identifier that allows the JACE to register its new IP address on the TZO servers. The JACE must register in one of two TZO domains (EasyIP.net or MyLinuxPC.com).



#### Notes

- The JACE-4/5 TZO client implementation will not work with the standard domains listed on the TZO web site (tzo.com, MyModem.com). If you want to use a TZO domain, you must use either EasyIP.net or MyLinuxPC.com. Be sure to specify this when you register with TZO.
- The TZO web site does not list the domain EasyIP.net, however you can still register your JACE in this domain.

TZO also offers several subscription packages with services in addition to DDNS. The services include domain registration and port forwarding. See the TZO web site ([www.tzo.com](http://www.tzo.com)) for more details.

### Registering with TZO

When you register with TZO you must contact them by telephone (not via web site) and specify:

- that you are an OEM customer
- that your host needs a name in either the EasyIP.net or MyLinuxPC.com domain
- an e-mail address they can use to contact you

You should receive the following information from TZO (see [Table 5-3](#)):

- A software key
- The [FQDN](#) of your JACE
- A list of the OEM update servers

## Configuring the JACE-4/5 for DDNS

The JACE-4/5 DDNS client set up in the `ddns.properties` file, which is accessible via the Admin Tool.

### About the `ddns.properties` file

The `ddns.properties` file includes four parameters, as listed in [Table 5-3](#). Just like the `ras.properties` file, parameters are listed in the form `<parameter>=<value>`. However, unlike the `ras.properties` file, several parameters are preceded by a pound sign, which you would need to remove to enable the parameter. For example, in [Figure 5-7](#), the `domainName` parameter has been enabled by the removal of the pound sign.

**Table 5-3** Parameters of the `ddns.properties` file.

| Parameter                                                                                    | Valid Values and Default Values (in Bold)                                                                                                                            | Description                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>enabled</code>                                                                         | <b>false</b><br>true                                                                                                                                                 | Set to true to enable the DDNS client. Since most JACEs do not require DDNS services, the default is false.                                                                                                                                                  |
| <code>domainName</code>                                                                      | a valid fully qualified host and domain name in the form:<br><code>&lt;name&gt;.&lt;TZOdomain&gt;.&lt;class&gt;</code>                                               | The fully qualified name of the JACE as given to you by TZO. For example:<br><code>domainName=JACE54.EasyIP.net</code><br><br><b>Note:</b> If you want to use a TZO domain, you must use either EasyIP.net or MyLinuxPC.com.                                 |
| <code>email</code>                                                                           | a string in the form:<br><code>&lt;username&gt;@&lt;domain&gt;.&lt;class&gt;</code>                                                                                  | The e-mail address given to TZO when you register.                                                                                                                                                                                                           |
| <code>key</code>                                                                             | any valid string including spaces                                                                                                                                    | This key, supplied by TZO, is sent by the JACE during each update. Enter exactly as it is given to you by TZO.                                                                                                                                               |
| <code>server1</code><br><code>server2</code><br><code>server3</code><br><code>server4</code> | any valid fully qualified server and domain name<br><b>OEMUpdate1.tzo.com</b><br><b>OEMUpdate2.tzo.com</b><br><b>OEMUpdate3.tzo.com</b><br><b>OEMUpdate4.tzo.com</b> | The servers that the JACE attempts to register the key with. It attempts to register with <code>server1</code> , and upon failure, tries the next server listed, and so on.<br><br><b>Note:</b> Be sure to verify these addresses with TZO when registering. |

### Configuring the `ddns.properties` file

Use the following steps to set up DDNS on the JACE:

#### Procedure 5-4 Configuring DDNS on a JACE-4/5.

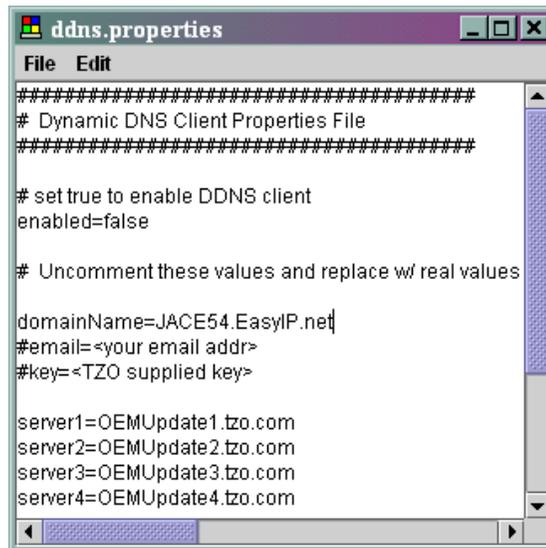
- Step 1** Using the **Admin Tool**, connect to and log into the JACE.
- Step 2** Click the **Network** tab.
- Step 3** Click **DDNS Properties**.

The `ddns.properties` file opens for editing ([Figure 5-7](#)).



#### Tip

If you do not see the DDNS Properties button, maximize the Admin Tool.

**Figure 5-7** ddns.properties file opened and in the process of being edited.

**Step 4** Edit the ddns.properties file using the information in [Table 5-3](#).

**Step 5** From the file menu, choose **File > Close**.

If you made any changes, you are prompted to save them, otherwise the window closes.

**Step 6** If prompted to save your changes, click one of the following:

- **Yes** to save your changes. The file saves and the window closes.
- **No** to discard your changes. The window closes.
- **Cancel** to return to the editing window, then refer to .

**Step 7** Reboot the JACE.

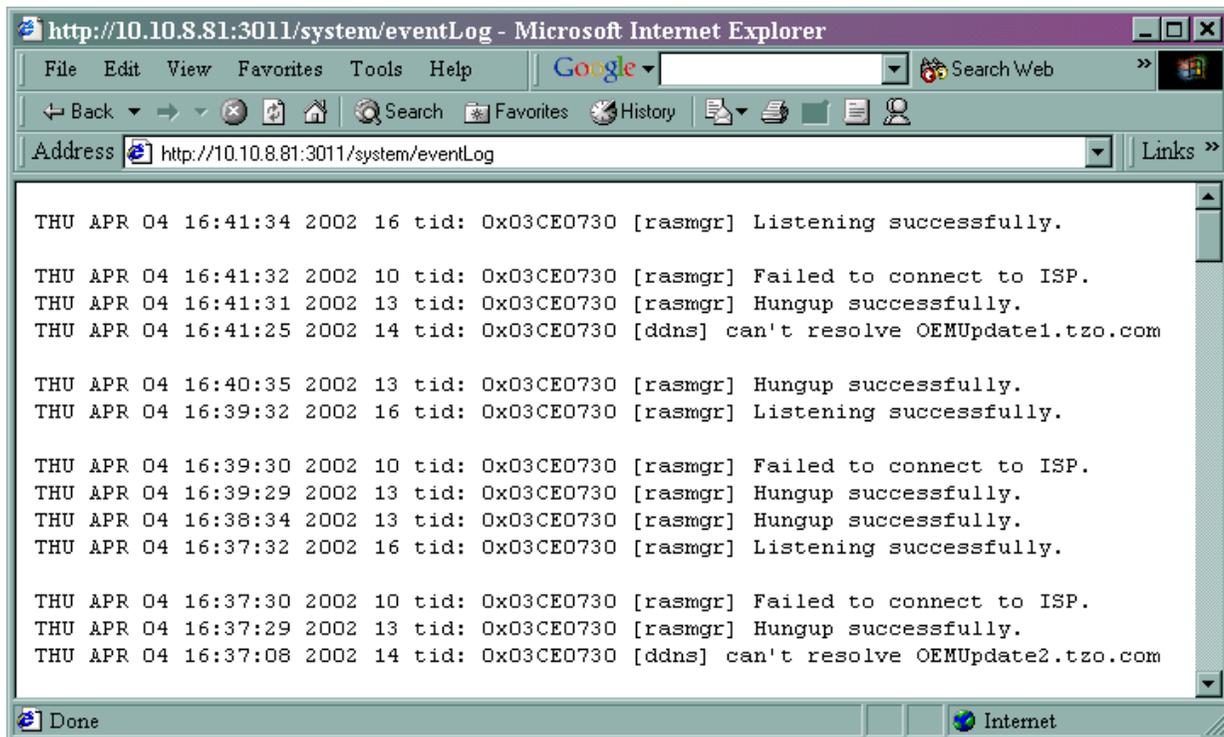
Assuming that RAS has been set up and tested on the JACE, the JACE automatically connects to the ISP and updates the DDNS server with its IP address. You can connect to the JACE using the domain name specified in the ddns.properties file.

## Troubleshooting DDNS Connections

As with troubleshooting captive ISP connections, troubleshooting DDNS connections requires a connection to the JACE via local LAN (over an IP connection) or by a serial connection. Errors in the DDNS update process are logged to the JACE-4/5 event log. The event log also contains the dynamic IP address assigned to the JACE upon reconnection to the ISP. You can access the event log via the Admin Tool (**Host > View Event Log**) or via a browser at `http://<host name or IP address>:3011/system/eventLog`.

[Figure 5-8](#) shows DDNS errors in the event log, as viewed via browser. The JACE cannot resolve the name of the TZO update servers when connected to the ISP. The problem was misconfigured DNS servers in the network settings of the JACE.

Figure 5-8 DDNS error in browser-view of event log.



In addition to the event log, you can try the following other techniques to diagnose problems after determining the IP address that the JACE is using.

- use `ping` and `tracert` to verify that you can ping that IP address from a remote workstation.
- use `nslookup` to query DNS servers at TZO to verify that the domain name assigned to the JACE is correctly mapped to the IP address assigned by the ISP.



#### Note

There is often a delay in the propagation of DNS changes. That may mean that the servers at TZO may have been updated, but the DNS servers that your workstation uses may not have updated. Use `nslookup` to query TZO and your DNS servers to pinpoint the discrepancy, then use the IP address information at TZO to connect to the JACE.

For more information on these troubleshooting commands, see the “[Connectivity Troubleshooting Utilities](#)” section on page 2-19.

## Troubleshooting Update Failures

If the JACE-4/5 is unable to update its DDNS entry, remote users will not be able to access it via domain name. It may be connected to the Internet, but its current address is unknown.

The JACE-4/5 treats an update failure in the same manner as an ISP connection failure. It hangs up the modem, waits and then retries again. If the update fails several times in a row, then the JACE reverts to dial-in mode. For more information on configuring the wait delays, retry counts, etc., see [Table 5-1](#) in the “[Configuring ras.properties for Captive ISP](#)” section on page 5-10.

## Connecting Windows-based Hosts via Telephone Modem

As mentioned in the “[Niagara Considerations](#)” section on page 5-1, you may be able to configure the Remote Access Server (RAS) on Windows-based Niagara hosts to dial an ISP. However, the following notes apply:

- RAS will not automatically redial on disconnect. That function must be provided by a third-party software application (such as RascalPro by Basta Computing).
- If the ISP assigns dynamic IP addresses, an Internet DDNS provider (TZO or other) must provide Windows-based client software to implement DDNS on these hosts.
- This scenario has not been tested by Systems Engineering. We recommend that you set up a pilot to test them before implementing in a live job.

This section provides a general overview of using RAS to connect to an ISP. To implement automatic redials and DDNS on your host, consult the documentation from the software vendors you choose for each function.



### Note

Be sure to review the information in the the “[Niagara Considerations](#)” section on page 5-1 for information on using NAT and proxies, selecting an ISP, and security considerations of attaching hosts directly to the Internet.

## Configuring the JACE-NP

These previous topics help you configure dial-up to an ISP on the JACE-NP.

- “[Installing and Configuring Modems](#),” page 4-17.
- “[Configuring the RAS Software](#),” page 4-20
- “[Granting Dial-in Permissions](#),” page 4-25

Work with your ISP to configure RAS to meet their network requirements.

## Configuring a Web Supervisor

These previous topics help you configure dial-up to an ISP on a Web Supervisor.

- “[Installing and Configuring Modems](#),” page 4-26.

- “Installing and Configuring the RAS Software,” page 4-27
- “Granting Dial-in Permissions,” page 4-31

Work with your ISP to configure RAS to meet their network requirements.

## Connecting via Cable or DSL Modem

As mentioned in the “Niagara Considerations” section on page 5-1, you may be able to use cable and DSL modems on Niagara hosts to dial an ISP. However, the following notes apply:

- With DSL or cable, the connection to the Niagara host is via the Ethernet connection, rather than the dial-up connection (as it is with a traditional modem). On a JACE-4/5 this means that the `ras.properties` and the `ispConnection` object (both used with the dial configuration) do not apply.
- Most cable and DSL connections are “always on” so there is little need to implement software that redials on disconnect. If necessary (when a dynamic IP address is assigned), DDNS can be implemented on JACE-NPs or Web Supervisor, but not on a JACE-4/5, as its DDNS implementation works on the dial interface only.
- Neither scenario has been tested by Systems Engineering. We recommend that you set up a pilot to test either before implementing in a live job.

**Note**

---

Be sure to review the information in the the “Niagara Considerations” section on page 5-1 for information on using NAT and proxies, selecting an ISP, and security considerations of attaching hosts directly to the Internet.

---

This section provides a general overview of configuring a cable or DSL connection to an ISP, as follows:

1. Install and configure the modem using the documentation provided by your vendor.
2. Using the Admin Tool, configure the network settings with the information provided to you by the ISP.
3. To implement automatic reconnect (if necessary) and DDNS on your host, consult the documentation from the software vendors you choose for each function.



## Using Security Technologies

---

This section discusses the issues associated with installing and using Niagara hosts in a secure environment. It has the following main topics:

- [Security Considerations](#)
- [Using a Firewall or Proxy Device](#)
- [Default Niagara Port Numbers](#)
- [Using a Virtual Private Network](#)

### Security Considerations

Any host connected to the Internet is vulnerable to attacks by someone else in the Internet community. This is especially true of any host that stays connected to the Internet virtually full time. Niagara hosts that may be vulnerable include:

- **Any Niagara host connected to a company's LAN and which has a public IP address.** The Web Supervisor shown in [Figure 3-1](#) and [Figure 3-2](#) is an example of one such host. Note that Company ABC has implemented a firewall on the LAN to lessen the vulnerability.
- **Any Niagara host directly connected to an ISP and which has a public IP address.** The hosts shown in sites 5 and 6 of [Figure 5-1](#) and most of the hosts in [Figure 5-2](#) meet this criteria.

Typically, Windows-based hosts are more vulnerable than JACE-4/5s. This is not a function of the Niagara software, but of two other factors:

- in Windows, there are many access points open by default that attackers can exploit. For a discussion of some of these, see [“Disabling Open Ports on Microsoft Windows NT 4.0,”](#) page 6-22. In contrast, the VxWorks OS has fewer access points enabled by default (although you can open some, see [“Guidelines for VxWorks-based Niagara Hosts,”](#) page 6-3).
- the widespread availability of the Windows OS itself. Because the VxWorks OS is less common, people have not taken the time to figure out how to attack it.

Another common point of attack for Internet hosts is the web server that runs on many Internet hosts (including Niagara hosts). However, our web server implementation is proprietary and not subject to the well-advertised attacks on Microsoft Internet Information Server and the Apache HTTP Server.

The following security suggestions are provided to help you secure Niagara hosts when connecting them to the Internet. You should evaluate the suggestions to see if they are applicable for each job that you architect.

**Note**


---

Many of these suggestions are also good guidelines for connecting hosts even in a LAN/WAN or direct-dial environment. Anyone with physical (or network) access to a host can be considered a security threat. You may want to consider implementing some of these, regardless of Internet connectivity.

---

### General Guidelines

- **Architect a LAN/WAN-only or LAN/WAN plus direct-dial solution**—The most obvious way to protect hosts is to avoid connecting them to the Internet at all. However, that limits connectivity from other hosts already connected to the Internet (typically BUI users or other Niagara hosts).
- **Implement a firewall between your Niagara host and the rest of the Internet community**—Firewalls provide a barrier between the Internet community and protected hosts. For more information, see the [“Using a Firewall or Proxy Device”](#) section on page 6-4.
- **Implement a VPN between Niagara hosts**—See [“Using a Virtual Private Network,”](#) page 6-23.
- **Implement strong passwords on each Niagara host and station**—Implementing strong passwords may prevent an attacker from guessing a Niagara host or station password. See [“Creating a Strong Password,”](#) page 6-3.
- **Change the default administrator password or establish a new administrator account on each host and delete or disable the default one that ships with the product**—Each JACE ships with at least one default host administrator user name and password (typically tridium/niagara). If you do not change or disable this account, any person familiar with our software can gain administrative access to the host.

**Caution**


---

If you change the password (or create a new account and disable the default), be sure to record your changes and store them in a place you (and your colleagues) can find them again. If you forget or lose the name or password you must ship the unit back for recovery.

---

- **Change the default HTTP port (and other ports)**—Changing server-side ports keeps out novice attackers, but may not stop more sophisticated ones. See [“Default Niagara Port Numbers,”](#) page 6-7 and [“Changing Niagara Default Ports,”](#) page 6-9.

## Guidelines for VxWorks-based Niagara Hosts

- **Do not enable FTP or telnet**—FTP and telnet are standard Internet protocols with well-documented attack points. If you must enable FTP or telnet on an VxWorks host, consider changing the port to keep the novice attacker out. This may not stop a more sophisticated attacker who uses port scanning software to learn about all the open ports on a host.

## Guidelines for Windows-based Niagara Hosts

- **Implement and maintain virus protection on any Web Supervisor that will connect to non-Niagara resources on the Internet**—If your Web Supervisor connects to other Internet resources (i.e., web pages, e-mail) you should implement and maintain virus protection. Viruses can make your Web Supervisor inoperable.
- **On a JACE-NP with the full version of the OS, stop the RCMD service and set its startup status to Manual**—RCMD provides command-line access by an administrator account to this model of JACE for maintenance purposes. It is a widely available Microsoft utility. However, if you stop RCMD and need to maintain the JACE-NP, you would need to attach a keyboard, mouse, and monitor to the device in order to maintain it.
- **Do not share folders on any Windows-based host**—Windows shares provide file-level access to the Windows host. Since they advertise themselves, once an attacker has deciphered a host password they are very vulnerable. If you must use Windows shares, make sure to assign permissions only to accounts using strong passwords.
- **Implement any security patches available from the OS vendor**—Be sure to periodically review and update patches when new vulnerabilities are patched. For more information on securing Windows-based hosts, see the Microsoft Security Resource Center at <http://www.microsoft.com/security/default.asp>.

For more information on securing hosts on the Internet, see <http://www.cert.org/>.

## Creating a Strong Password

The best secure password is difficult to guess and difficult to crack, but easy for you to remember. To provide the highest level of security, the password should challenge password cracking software so that it takes more time to crack than most people would be willing to devote to it.

The following types of passwords are insecure because they are easy to guess by people you know or easy to crack by people you do not know:

- Any word, common or not, even one in a foreign language
- Any name (yours, your spouse or children, your boss, your pet)
- Any password made up of all numbers (bank card number, house numbers, telephone numbers, US Social Security number, or car license plate number)

A secure password should contain at least **three** of the following elements:

- Have at least eight characters (the more characters, the longer it takes to crack)
- Have both upper and lower case letters
- Contain both letters and numbers
- Contain special characters (interspersed between letters and numbers)

In addition, a secure host password should also be easy for you to remember so that you are not tempted to write it down and leave it in an insecure area (such as taping it to the unit). As mentioned in the previous section it **is** a good idea to note any password (or name) that you create or change and keep it in a secure area that is still accessible to the rest of your team members.

So how do you create a strong password that is easy to remember, but follows the guidelines listed above? One common method entails swapping out alphabetic characters with numeric or special-character equivalents. For example:

- the word `baseball` becomes `b@s3B@11`
- the phrase `playmahjong` becomes `p!@yM@4j0nG`

Fortunately, the Niagara software has a strong password feature to help you enforce secure passwords at the station level (for more information, refer to the section about the Station object in Chapter 1 of the *Niagara Standard Programming Reference*). However, for host passwords, you will have to remember to create secure passwords on your own.

## Using a Firewall or Proxy Device



### Notes

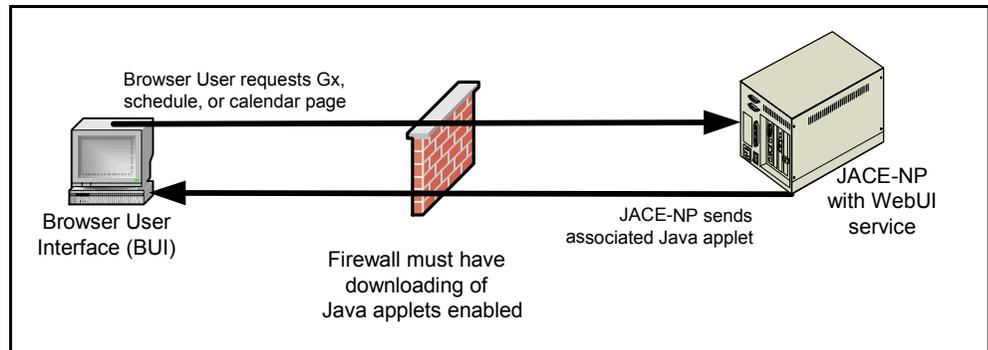
- If you have not already done so, please review the “[Proxy Servers and Firewalls](#)” section on page 1-28 to familiarize yourself with the various techniques used by firewalls and proxy servers.
- Working with these devices can be confusing because many devices that are labelled for one function (such as “firewall”) also can provide other functionality as well (such as proxy functions). Therefore, if you encounter an existing device (be it a router, firewall or proxy server), you should investigate the functions that it provides for the organization.
- You should consult the system owner’s IT department on these issues during the planning phase of the installation to avoid unnecessary delays and rework resulting from a lack of adequate communication.

The system architecture figures throughout this book ([Figure 3-1](#), [Figure 3-2](#), [Figure 4-1](#), [Figure 4-2](#), [Figure 5-1](#)) provide typical examples of Niagara hosts in use with a corporate firewall. In those examples, the equipment in sites 1–4 is behind a firewall, but equipment at sites 5 and 6 is not.

Niagara hosts function well in many firewall environments, with the following conditions:

- Java applets must be able to be downloaded through the firewall. Any Niagara host serving up GxPage graphics, log charts, and schedule and calendar editors must be able to send the applets associated with these servlet pages to a BUI client. (Figure 6-1).

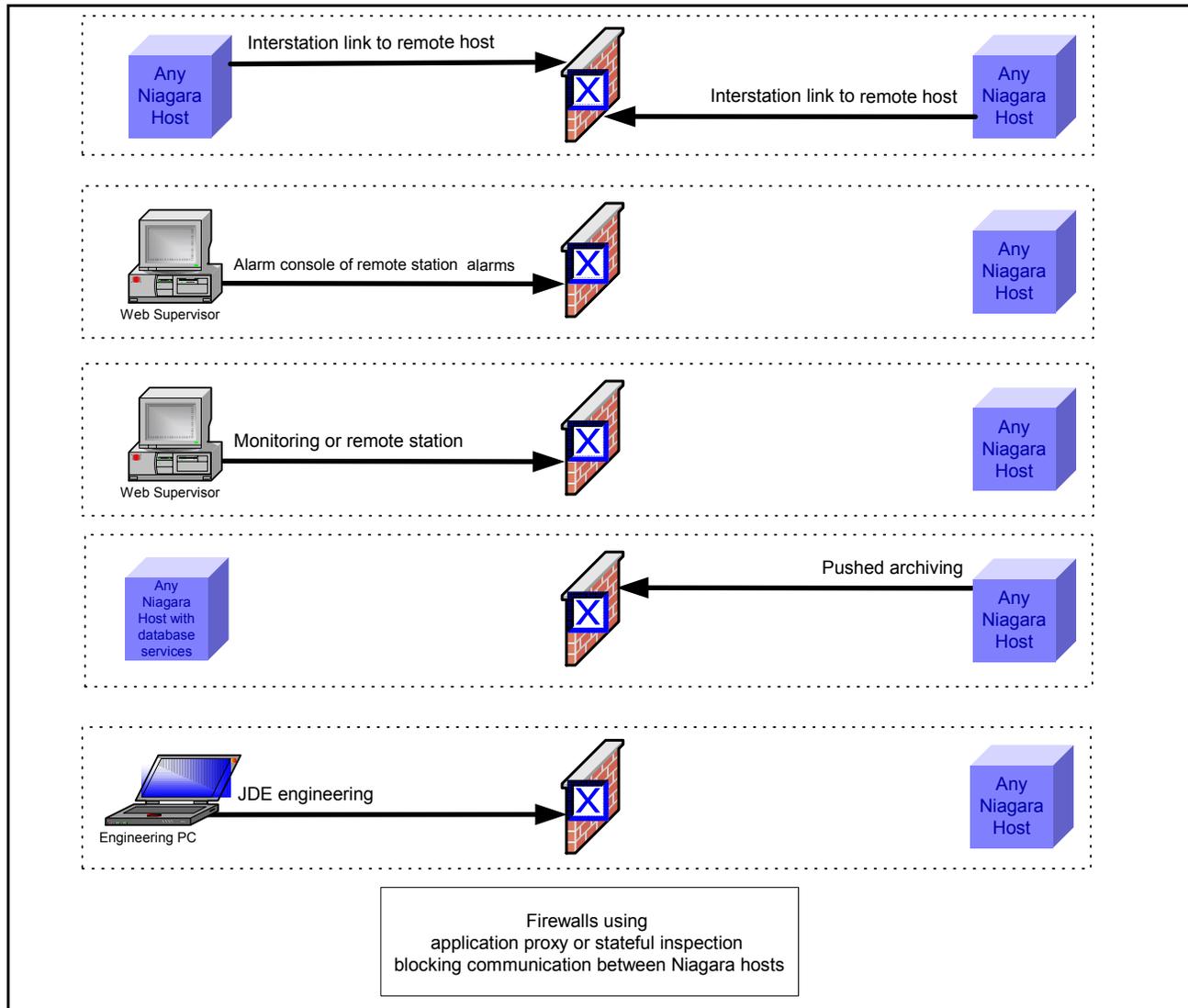
**Figure 6-1** Java applet downloading to a BUI client through a firewall.



- On any firewall, application ports may need to be opened to allow communication between any two Niagara hosts on opposite sides of the firewall. See the “[Default Niagara Port Numbers](#)” section on page 6-7.
- Firewalls using the *application proxy* and *stateful inspection* techniques for security may block the following Niagara communication functions (see [Figure 6-2](#)):
  - using interstation links between stations
  - using the alarm console to monitor alarms on a remote station
  - using the station monitoring function to monitor a remote host
  - using pushed archiving
  - using the JDE to engineer a remote station

These connections are created using an HTTP request to open a socket. Once the socket is open the connection remains open and proprietary messages are sent between the server and client (without the appropriate HTTP header). Any technique that inspects each packet for validity may reject these successive packets. If you require these functions, request that the firewall be configured to not block connections between Niagara hosts.

Figure 6-2 Types of Niagara communication blocked with an application proxy or stateful inspection firewall.



The following communication functions between hosts separated by a firewall **will** work, even when the firewall uses application proxy and stateful inspection:

- browser to station
- Admin Tool to host
- polled archiving
- time synchronization

For a description of any of these communication functions, see the [“Communication between Niagara Hosts”](#) section on page 1-35.

If you are implementing a firewall in lieu of using one already in place, a good security practice is to grant the most limited permissions you can on the firewall, while still following the guidelines for communication listed above.

# Default Niagara Port Numbers



**Note** If you are unfamiliar with the role application ports play in Internet communications, please review the [“About Ports”](#) section on page 1-31.

As with most Internet-enabled applications, the applications running on Niagara hosts also use default ports for communication with clients (typically other Niagara hosts, or BUI users). For instance:

- a browser client that connects to a GxPage does so on port 80 of a Niagara host running WebUI services.
- an engineering PC (the client) uses JDE to connect to a station for maintenance, also on the station’s server port 80.
- an engineering PC (the client) uses the Admin Tool to change an IP address on the host, and connects on the host’s server port 3011.

[Table 6-1](#) table provides a list of the types of communication used by Niagara hosts, and the default server ports used. Unless otherwise noted:

- the client randomly chooses an available client-side port (1024 or greater) to talk to the listed server port
- the server port listed is a TCP port (rather than a UDP port)
- most of the ports in the table are constantly open. Some applications (such as FTP, or our web server) constantly keep a port open, which means the port is scannable by a port scanner. Other ports (such as the host Admin port) only are shown when they are in use.

For a description of the communication functions listed in [Table 6-1](#), see the [“Communication between Niagara Hosts”](#) section on page 1-35.

**Table 6-1 Communication between Niagara hosts and the default server port used.**

| Communication                  | Client         | Server           | Default Server Port                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|----------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Browser User Interface (BUI)   | Any host       | Any Niagara host | <ul style="list-style-type: none"> <li>• 80—to access Gx, chart, calendar and schedule pages and station administration servlet pages (for a description of these, see <a href="#">“Changing the Station HTTP Port (80),”</a> page 6-9).</li> <li>• 3011<sup>1</sup>—to access host-based administration pages (for a description of these, see <a href="#">“Changing the Administration Port (3011),”</a> page 6-12).</li> </ul> |
| Java Desktop Environment (JDE) | Engineering PC | Any Niagara host | 80                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Default Niagara Port Numbers

**Table 6-1** Communication between Niagara hosts and the default server port used.

| Communication                              | Client                                                                      | Server                                                             | Default Server Port                                                                                                                                                                                                                                                                           |
|--------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Tool                                 | Engineering PC                                                              | Any Niagara host                                                   | <ul style="list-style-type: none"> <li>• 3011—for most host-based functions (like changing network settings)</li> <li>• 80—for station functions such as backing up the station, version upgrades and converting the database to a different format.</li> </ul>                               |
| NetMeeting                                 | Windows PC or JACE-NP                                                       | JACE-NP (Embedded NT)                                              | <ul style="list-style-type: none"> <li>• 389—Internet Locator Service (ILS)</li> <li>• 522—User Location Service</li> <li>• 1503—T.120</li> <li>• 1720—H.323 call setup</li> <li>• 1731—Audio call control</li> <li>• Dynamic—H.323 call control and streaming</li> </ul> (all <sup>1</sup> ) |
| RCMD                                       |                                                                             | JACE-NP (Full NT)                                                  | <ul style="list-style-type: none"> <li>• 139 (server)</li> <li>• 2770 (client)</li> </ul>                                                                                                                                                                                                     |
| Telnet                                     | Windows PC or JACE-NP                                                       | JACE-4/5                                                           | 23 (TCP and UDP)                                                                                                                                                                                                                                                                              |
| FTP                                        |                                                                             |                                                                    | 21 (TCP and UDP)                                                                                                                                                                                                                                                                              |
| Hyperterminal                              |                                                                             |                                                                    | <ul style="list-style-type: none"> <li>• None—when used to attach directly to a COM port.</li> <li>• 23—when used as a telnet client.</li> </ul>                                                                                                                                              |
| Pushed archiving                           | Any Niagara host                                                            | JACE-NPs and Web Supervisors running the Database service          | 80                                                                                                                                                                                                                                                                                            |
| Polled archiving                           | JACE-NPs and Web Supervisors running the Database and Poll Archive services | Any Niagara host                                                   | 80                                                                                                                                                                                                                                                                                            |
| Alarm archiving                            | Any Niagara host with notification set to archive_remote                    | JACE-NPs and Web Supervisors running the Database service          | 80                                                                                                                                                                                                                                                                                            |
| Alarm e-mail notification                  | Any Niagara host running the Mail service.                                  | Any SMTP mail server                                               | 25                                                                                                                                                                                                                                                                                            |
| Remote printer notification                | Any Web Supervisor or JACE-NP                                               | Any networked printer                                              | 135 (for RPC connectivity), 139<br>UDP: 137, 138                                                                                                                                                                                                                                              |
| Alarm Console acknowledgement              | Web Supervisor or any engineering PC                                        | A Niagara host with alarming set up to archive local               | 80                                                                                                                                                                                                                                                                                            |
| Time synchronization                       | Any Niagara host with the TimeSync Service                                  | Any Internet Time Protocol server (including another Niagara host) | 37 <sup>1</sup>                                                                                                                                                                                                                                                                               |
| Backup subordinate                         | Supervisor station                                                          | Subordinate station                                                | 80                                                                                                                                                                                                                                                                                            |
| Global data passing via interstation links | Any Niagara host                                                            | Any Niagara host                                                   | 80                                                                                                                                                                                                                                                                                            |
| Station monitor                            | Supervisor station                                                          | Any Niagara host                                                   | UDP: 80                                                                                                                                                                                                                                                                                       |

1. Port is hidden until used.

## Changing Niagara Default Ports

You will note that most connections between Niagara hosts listed in the previous table occur on the default HTTP port of 80, or the host administration port of 3011. Both of these ports can be changed in our application. You can also change the server port of any Niagara host acting as a time synchronization server. Typically, you do not need to change these ports but you may choose to do so for security or other reasons.

Changing these default ports is discussed in the following sections:

- [Changing the Station HTTP Port \(80\)](#)
- [Changing the Administration Port \(3011\)](#)
- [Changing the Time Synchronization Port](#)

### Changing the Station HTTP Port (80)

As referenced in [Table 6-1](#), the JDE and many interstation processes use port 80 for communications. This port is also used by:

- browser users to access Gx pages and station administration pages (those requiring a station-based login), such as:
  - `http://<host_name>/`
  - `http://<host_name>/chart/log`
  - `http://<host_name>/prism`
  - `http://<host_name>/db`
  - `http://<host_name>/alarm`
- the Admin Tool for functions such as:
  - DBadmin functions
  - release upgrades
  - station backups
- the station monitor (on UDP port 80)

Changing the default HTTP port of the station is a two step process:

- [Changing the HTTP Port of the Station](#)
- [Changing the HTTP Port used by the Admin Tool for Station Functions](#)

### Changing the HTTP Port of the Station

#### Procedure 6-1 Changing the HTTP port of the station.

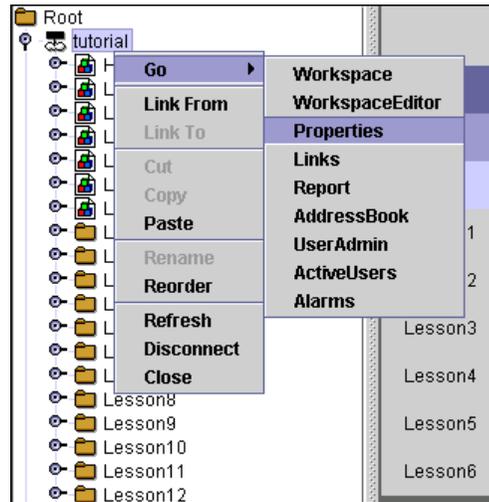
**Step 1** In the JDE, open the station on which you want to change the HTTP port.

**Step 2** In the tree view, right-click the station and select **Go > Properties**.

The properties sheet of the station opens.

[Figure 6-3](#) provides an example of this step being performed on the tutorial station of a Web Supervisor.

Figure 6-3 Menu navigation to change HTTP port.



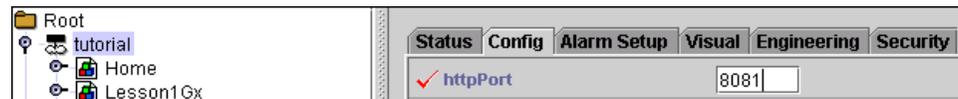
**Step 3** On the properties sheet, click the **Config** tab.

**Step 4** Edit the **httpPort** text box, removing the default port of 80 and replacing it with your chosen port number (such as 8081). See Figure 6-4.

**Tip**

Many ports are assigned to other TCP/IP applications. To avoid a conflict, see <http://www.iana.org/assignments/port-numbers> for a full list of registered and well known ports.

Figure 6-4 Config tab and httpPort text box with new port.



**Step 5** Click **Apply**.

**Step 6** Using the Admin Tool, stop and start the station (or reboot the host) and verify that the station is running.

Your change is enabled in the station.

**Step 7** Test the functionality of the new port by connecting to the station with a browser. You must use the new port number in the URL. For example:

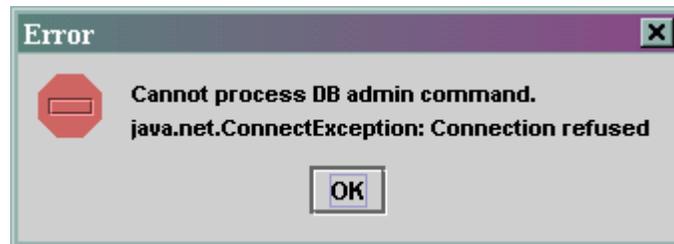
```
http://<hostname>:8081/
```

where *<hostname>* is the name or IP address of the host with the station you changed. See also “Impact of Changing Default Niagara Ports,” page 6-18.

## Changing the HTTP Port used by the Admin Tool for Station Functions

When you change the station HTTP port, the Admin Tool will no longer be able to connect to the station to perform station functions. [Figure 6-5](#) provides an example of the type of error you might encounter if you change the HTTP port in the station but fail to make the appropriate change for the Admin Tool.

**Figure 6-5** Admin Tool DBAdmin error after changing HTTP port in station properties.



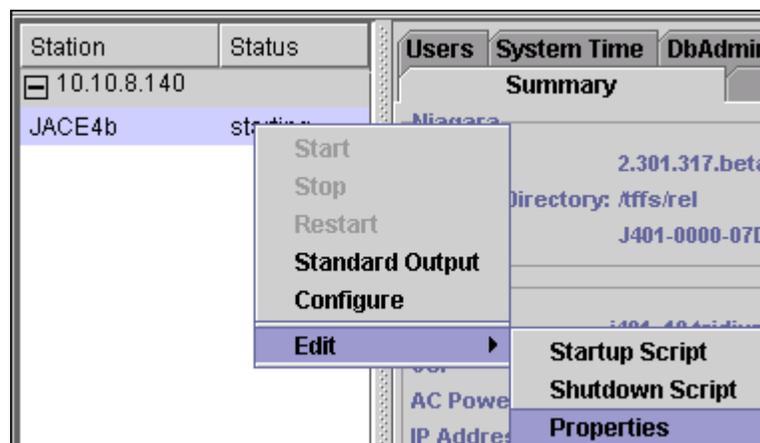
In order to correct this, you must add a line in the station.properties file that references the new port number. You can edit this file using the Admin Tool, as follows:

### Procedure 6-2 Changing the HTTP port used by the Admin Tool for station functions.

- Step 1** If you have not already done so, open the Admin Tool and log into the host that contains the station that you changed in the previous procedure.
- Step 2** Right-click the station name (not the host name or address) and select **Edit > Properties** ([Figure 6-6](#)).

The station.properties file opens for editing in a new window.

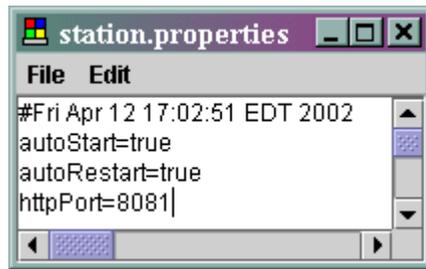
**Figure 6-6** Opening the station.properties file in the Admin Tool.



- Step 3** Add a line to the file that reads:

```
httpPort=<newport>
```

where *<newport>* is the same port that you used in [Step 4](#) of the previous procedure. Be sure to type in the line with the capitalization as shown. See [Figure 6-7](#).

**Figure 6-7** station.properties file with added httpPort information.

- Step 4** From the file menu, choose **File > Close**.
- If you made any changes, you are prompted to save them, otherwise the window closes.
- Step 5** If prompted to save your changes, click one of the following:
- **Yes** to save your changes. The file saves and the window closes.
  - **No** to discard your changes. The window closes.
  - **Cancel** to return to the editing window, then refer to [Step 3](#).
- Step 6** To enable the change, stop and start the station and verify that it is running.
- Step 7** Test the functionality of your new port by initiating a database conversion (refer to the Administration Tool section of the *TCP Student Guide* for information on this step). If you receive an error like the one shown in [Figure 6-5](#), verify that you added the `httpPort` line correctly.
- 

## Changing the Administration Port (3011)

As referenced in [Table 6-1](#), the Admin Tool connects to a Niagara host on port 3011 for most administration functions. This port is also used by browser users to access station administration pages. These include any page that references the default administration (admin) port of 3011 (and which requires a host-based login), such as:

- `http://<host_name>:3011`
- `http://<host_name>:3011/system/spy` (JACE-4/5 only)
- `http://<host_name>:3011/system/eventLog` (JACE-4/5 only)

To change this administration port, you must add a line to the `niagrad.properties` file. This file is located in `<current_release_directory>\nre\lib` of any Niagara host (you may have to create this file on Windows-based hosts).

### Determining the Current Release Directory

Depending on the host platform, the location of the current release directory changes. Use the following steps to determine the current release directory.

#### Procedure 6-3 Determining the current release directory of any Niagara host.

---

- Step 1** Using the Admin Tool, open the host on which you want to make the port change.

- Step 2** On the **Summary** tab, make note of the path listed in the **Release Directory** field. This is the current release directory.
- 

Neither the Admin Tool nor the JDE provide a mechanism to add or edit the `niagarad.properties` file; instead you must use one of the following procedures to manually create or edit the file as needed:

- [Changing the Admin Port on a Web Supervisor](#)
- [Changing the Admin Port on a JACE-NP](#)
- [Changing the Admin Port on a JACE-4/5](#)



**Caution** Do not alter the existing content of `niagarad.properties`. Only add the information described in the following procedure.

---

## Changing the Admin Port on a Web Supervisor

### Procedure 6-4 Changing port 3011 of a Web Supervisor host.

---

- Step 1** On the Web Supervisor, open the Windows text editor **Notepad** by selecting **Start > Programs > Accessories > Notepad**.
- Step 2** From the menu, choose **File > Open**.
- The **Open** dialog box appears and is initially set to show only files with a `.txt` extension.
- Step 3** In the **Open** dialog box, change the **Files of Type** list to **All Files**.
- Step 4** Using the current release directory information you noted in [Step 2](#) of the previous procedure, browse the drive (and the sub-directories) to locate the `niagarad.properties` file.

A typical directory and file structure looks like this:

```
D:\niagara\r2.203.nnn\nre\lib\niagarad.properties
```

- Step 5** If you find the file, double-click to open it. Otherwise, click **Cancel** to be returned to the new (untitled) file window.
- Step 6** Add a line to the file that reads:

```
adminPort=<newport>
```

where `<newport>` is the number of the new port. Be sure to type in the line with the capitalization as shown. [Figure 6-8](#) shows an example of the line added to a new (not yet saved) `niagarad.properties` file.

**Figure 6-8** Changing the admin port in a niagarad.properties file.**Tip**

You can add comment lines to any Niagara text file with the use of preceding # characters, as shown in [Figure 6-8](#). It is a good idea to add comments about any changes you make to a file in case you (or someone else) need to reverse them later.

- 
- Step 7** From the menu, choose **File > Save**. The **Save** dialog box opens.
- Step 8** Verify that you are still in the `\nre\lib` directory.
- Step 9** If saving a previously created `niagarad.properties` file, click **Save**, and overwrite the existing file. Otherwise, if saving a newly created file:
- a. In the **Save** dialog box, change the **Save as type** list to **All Files**.  
If you do not execute this step, your file saves with a `.txt` extension and the system ignores it.
  - b. In the **File name** text box, type:  
`niagarad.properties`
  - c. Click **Save**.
- Step 10** Reboot the host to enable the change.
- Step 11** Verify connectivity to the host by connecting to it using the Admin Tool. Be sure to reference the new port number in the **Connect to Host** dialog box (see [“Impact of Changing Default Niagara Ports,”](#) page 6-18).
- 

## Changing the Admin Port on a JACE-NP

### Procedure 6-5 Changing port 3011 of a JACE-NP host.

- 
- Step 1** Access the desktop of the JACE-NP with either a keyboard, monitor and mouse (Full) or NetMeeting (Embedded). For instructions on how to use NetMeeting, see the [“NetMeeting”](#) section on page 2-2.
- Step 2** Click **Start > Run**.
- Step 3** In the text box, type:  
`notepad`  
The Windows Notepad application opens.

**Step 4** Follow [Procedure 6-4](#) from [Step 2](#).

---

Alternately, you can use one of the two following methods to add or edit the `niagarad.properties` file:

- browse the network and locate the JACE-NP. Double-click the **niagara** share (logging in, if necessary), then change directories to the current release directory, and the **nre\lib** subdirectory. Open the file (or add it) with Notepad as described previously.
- using RCMD, connect to a JACE-NP Full. Change drives and directories to the current release directory, and the **nre\lib** subdirectory. Copy the file (if it exists) to your local PC. Edit the file (or create it) and copy the file back to the **nre\lib** subdirectory of the JACE.

### Changing the Admin Port on a JACE-4/5

With the JACE-4/5, you cannot edit the file in place as you can with the Windows hosts. You must use FTP to transfer the file to your local PC, then edit it locally, and transfer it back, as follows:

#### Procedure 6-6 Changing port 3011 of a JACE-4/5 host.

---

**Step 1** Using an FTP application, connect and log into the JACE-4/5. (For instructions on how to use the Windows command-line FTP application, see the “[FTP](#)” section on page 2-17.)

**Step 2** Transfer a copy of the `niagarad.properties` file to your local PC, as follows:

- a. Change to the **/nre/lib** subdirectory of the current release directory (see [Procedure 6-3](#)) of the JACE. If you are using command-line FTP, type:

```
cd /<current_release>/nre/lib
```

Be sure to include the `/` character before the path. Typically, you would type something like the following:

```
/tffs/rel/nre/lib
```

```
/sm/rel/nre/lib
```

- b. Verify that the `niagarad.properties` file is in this directory. If you are using command-line FTP, type the list files command:

```
ls
```

- c. Set the local directory on your PC to the `<x>:\niagara` directory (or another of your choosing). In command-line FTP, type:

```
lcd <x>:\niagara
```

where `<x>` is the drive on which the `niagara` directory resides.

- d. Set the file transfer type to binary. In command-line FTP, type:

```
bin
```

- e. Copy the file to your local PC. In command-line FTP, type:

```
get niagarad.properties
```

In command-line FTP, these steps will look similar to [Figure 6-9](#).

**Figure 6-9** Using FTP to transfer a file off of a JACE-4/5.

```

C:\>ftp 10.10.8.140
Connected to 10.10.8.140.
220 UxWorks (5.4.2) FTP server ready
User (10.10.8.140:(none)): tridium
331 Password required
Password:
230 User logged in
ftp> cd /tffs/rel/nre/lib
250 Changed directory to "/tffs/rel/nre/lib"
ftp> ls
200 Port set okay
150 Opening ASCII mode data connection
.
..
license.properties
comm.jar
drivers.properties
nre.jar
mime.properties
niagarad.properties
gx.properties
226 Transfer complete
ftp: 111 bytes received in 0.00Seconds 111000.00Kbytes/sec.
ftp> lcd d:/niagara
Local directory now D:\niagara.
ftp> bin
200 Type set to I, binary mode
ftp> get niagarad.properties
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 20 bytes received in 0.00Seconds 20000.00Kbytes/sec.
ftp> _

```

- Step 3** Edit the file with the Windows Notepad application, as described in steps 1–9 of [Procedure 6-4](#). In this instance, you will not find the file in the current release directory, but rather in the <x>:\niagara directory (or whichever download directory you chose).
- Step 4** Transfer the edited file back to the JACE-4/5, as follows:
- a. If your FTP session with the JACE has timed out, refer to [2](#), substeps a–d to get the session set back up.
  - b. Copy the niagarad.properties file from your local PC back to the JACE. In command-line FTP, type:
 

```
put niagarad.properties
```

In command-line FTP, these steps will look similar to [Figure 6-10](#).

Figure 6-10 Using FTP to copy a file to a JACE-4/5.

```

C:\WINNT\System32\cmd.exe - ftp 10.10.8.140
Local directory now D:\niagara.
ftp> bin
200 Type set to I, binary mode
ftp> get niagarad.properties
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 20 bytes received in 0.00Seconds 20000.00Kbytes/sec.
ftp> put niagarad.properties
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 36 bytes sent in 0.00Seconds 36000.00Kbytes/sec.
ftp>

```

- Step 5** Reboot the JACE.
- Step 6** Verify connectivity to the host by connecting to it using the Admin Tool. Be sure to reference the new port number in the **Connect to Host** dialog box (see [“Impact of Changing Default Niagara Ports,”](#) page 6-18).

## Changing the Time Synchronization Port

With time synchronization, one host can receive updates to its system time from another host. A Niagara host can function as both a time synchronization client and a time synchronization server. Niagara hosts can also use Internet time synch servers for system time updates.

When acting as a server, a Niagara host can be contacted on port 37 (the “well known” time synchronization port) by any time synchronization client. You can change this default port on the properties sheet of the TimeSyncService (see [Procedure 6-7](#) for detailed instructions).



### Note

If you change the default server port, other hosts looking to this time server for synchronization must contact the host on the new port. For instructions on how to configure a Niagara client to use the new port, see [“Changing the time synchronization port a Niagara client uses to contact a server,”](#) page 6-20.

### Procedure 6-7 Changing the default time synchronization port.

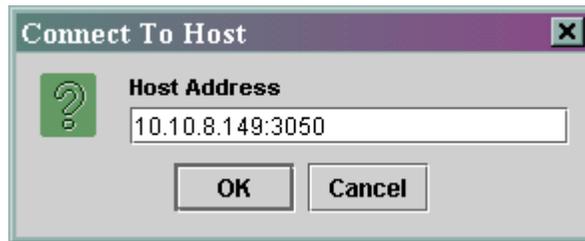
- Step 1** Using the JDE, open the station for which you want to change the time synchronization port.
- Step 2** In the tree view, expand the **services** container.
- Step 3** Right-click the **TimeSyncService**, and choose **Go > Properties**.
- Step 4** Click the **Config** tab.
- Step 5** Edit the **serverPort** text box, removing the default port of 37 and replacing it with your chosen port number.

- Step 6** Click **Apply**.
- Step 7** Using the Admin Tool, stop and start the station (or reboot the host) and verify that the station is running.
- Your change is enabled in the station.
- Step 8** Verify that a time synchronization client correctly updates its system time.

## Impact of Changing Default Niagara Ports

When using the default HTTP and Admin port, you do not need to specify them in the application. However, after changing either port, you need to specify the new port in any instance of communicating with the host. In most cases, you append the port (with a preceding colon) to the end of the host name or IP address. [Figure 6-11](#) provides an example of using the Admin Tool to open a session to a host (10.10.8.149) with a changed Admin port (3050).

**Figure 6-11** Specifying the port when connecting to a host with a changed admin port.



Once you connect to the host, the changed port is shown wherever the host name or IP address is shown. [Figure 6-12](#) shows an example of the previous host open in the Admin Tool.

**Figure 6-12** Changed admin port showing in the Admin Tool.

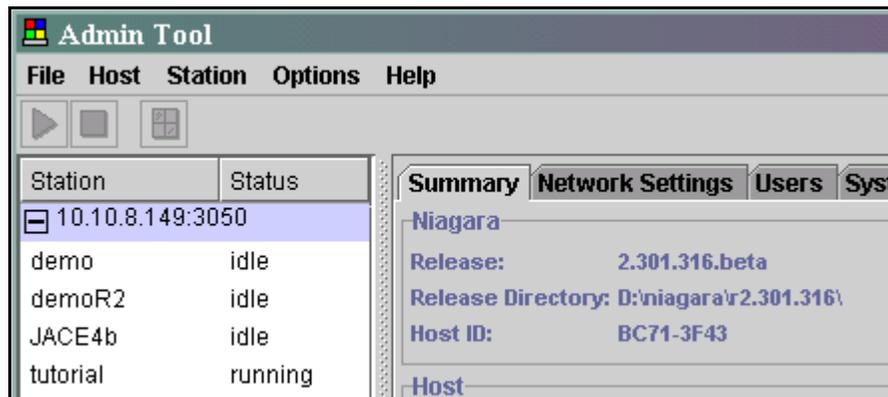
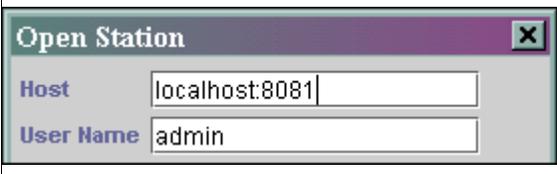
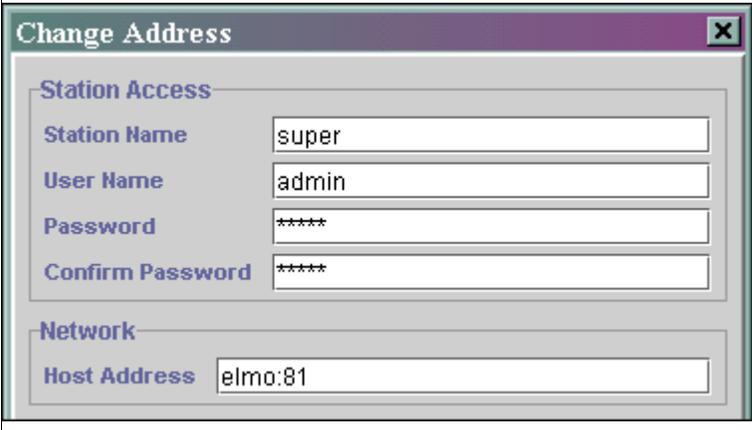
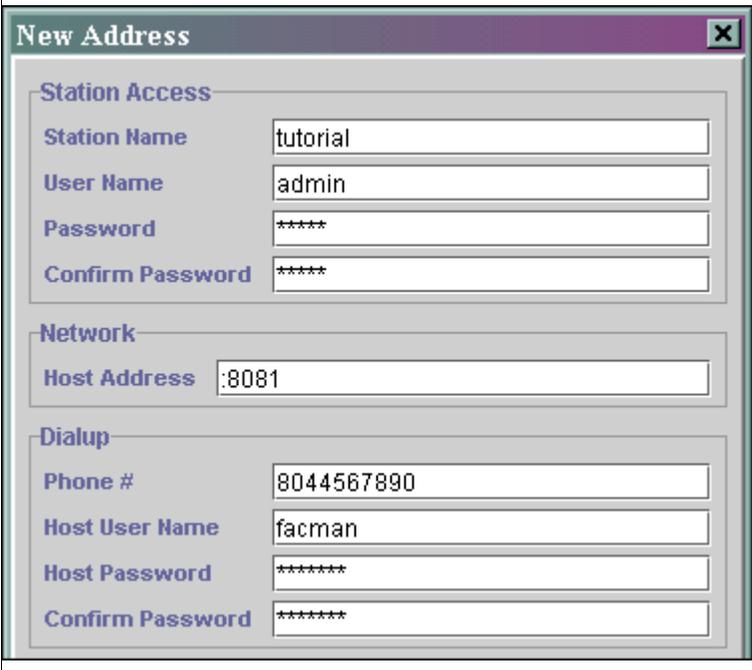
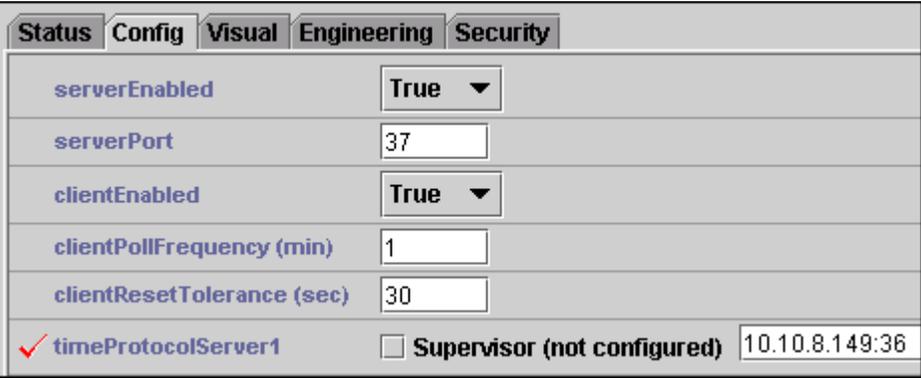


Table 6-2 provides other selected instances where you also need to specify the new port along with the host name or IP address.

**Table 6-2 Selected examples of specifying a port after a port change.**

| Action                                                                           | Example                                                                              |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Opening a station with a changed HTTP port.                                      |    |
| Adding an address book entry for a host on the network with a changed HTTP port. |    |
| Adding an address book entry for a dial-up host with a changed HTTP port.        |  |

**Table 6-2** Selected examples of specifying a port after a port change. (continued)

| Action                                                                                                                                                                                                                                                                                                                       | Example                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <p>Changing the time synchronization port a Niagara client uses to contact a server.</p> <p><b>Note:</b> If you use the Supervisor check box, the application tries to contact its Supervisor on the default port of 37. To contact the Supervisor (or any other time synch host) on another port, use the method shown.</p> |   |
| Connecting to a GxPage on a station with a changed HTTP port.                                                                                                                                                                                                                                                                |   |
| Connecting to a host-based page on a host with a changed Admin port.                                                                                                                                                                                                                                                         |  |

## Additional Open Ports on the JACE-NP

When you install a factory-fresh JACE-NP, several additional well known server ports are, by default, open and scannable. They are listed in [Table 6-3](#), by the model and function:

**Table 6-3** Additional default (non-Niagara) ports.

| Platform              | Port | Function                                                                                                                                                                                                                                       |
|-----------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Embedded JACE-NP only | 7    | Echo—RFC 862. Once a a client establishes a connection, any data received by the server is sent back to the client. This continues until the client terminates the connection.                                                                 |
|                       | 9    | Discard—RFC 863. Once a client establishes a connection, any data received by the server is thrown away. No response is sent. This continues until the client terminates the connection.                                                       |
|                       | 13   | Daytime—RFC 867. Once a client establishes a connection, the current date and time is sent out on the connection as a ascii character string (and any data received is thrown away). The service closes the connection after sending the data. |

**Table 6-3 Additional default (non-Niagara) ports.**

| Platform                         | Port | Function                                                                                                                                                                                                                         |
|----------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Embedded JACE-NP only, continued | 17   | QOTD (quote of the day)—RFC 865. Once a client establishes a connection, a short message is sent out on the connection (and any data received is thrown away). The service closes the connection after sending the quote.        |
|                                  | 19   | Chargen (character generator)—RFC 864. Once a client establishes a connection, a stream of data is sent out on the connection (and any data received is thrown away). This continues until the client terminates the connection. |
| Embedded and Full JACE-NPs       | 135  | epmap—Microsoft RPC end-point mapper. Used by a number of Windows intercommunication process. See Microsoft Knowledge Base article Q150543 for details. <sup>1</sup>                                                             |
|                                  | 139  | netbios-ssn—Microsoft NetBIOS session service. Used by a number of Windows intercommunication process. See Microsoft Knowledge Base article Q150543 for details. <sup>1</sup>                                                    |

1. <http://support.microsoft.com/default.aspx?scid=kb:en-us:Q150543>

**Note**

Ports 135 and 139 are standard open Windows ports. Therefore, they are likely to be open on any Windows-based host, such as a Web Supervisor or engineering PC.

There are known security vulnerabilities with TCP and UDP ports 135 through 139. However, because they are used by many Microsoft functions, it may not be advisable to disable. Disabling them may mean that other functions (as listed in the Knowledge Base article) may fail to work. For the best security, these hosts should be located behind a packet filtering or other firewall device and access to these ports should be restricted.

However, if you cannot locate the hosts behind a firewall you can disable most of the open TCP ports without impacting Niagara or host administration functions. For our application to function you must leave the following TCP server ports open on the JACE-NP:

- 80 (or whichever HTTP port you use for station functions.)
- UDP: 80 (if you are using the station monitoring function)
- 3011 (or whichever Admin port you use for host administration functions)
- 37 (if using the host as a time synchronization server)
- TCP: 135, UDP 137, 138 (if this host is acting as a Windows print server for other hosts)
- 139 (if using RCMD on a Full JACE-NP, or host is acting as a Windows print server)
- 1503 (for NetMeeting—Embedded JACE-NPs only)

**Note**

It is a good idea to test disabling the ports in a controlled environment before placing equipment in the field. You may find, depending on the ISP setup, that you need to enable some ports when you get the equipment to the field.

## Disabling Open Ports on Microsoft Windows NT 4.0

Use the following procedure to enable only those ports (Niagara and other) that you require:

### Procedure 6-8 Disabling open ports.

- 
- Step 1** Access the desktop of the JACE-NP with either a keyboard, monitor and mouse (Full) or NetMeeting (Embedded). For instructions, see “[NetMeeting](#),” page 2-2.
- Step 2** On the desktop, right-click the **Network Neighborhood** icon and select **Properties**.
- Step 3** Click the **Protocols** tab, then double-click **TCP/IP Protocol**.  
The TCP/IP Properties dialog box opens.
- Step 4** On the **IP Address** tab, click **Advanced**.
- Step 5** Click the **Enable Security** check box, and then click **Configure**.
- Step 6** In the **TCP Ports** area, click **Permit Only** and click **Add**.
- Step 7** Type the number of a port that you want to enable on this host, and click **Add**.
- Step 8** Repeat steps 8–9 until you have added all the TCP ports you wish to enable.



#### Caution

If you leave the TCP list blank, **all** port connections of that type are disabled (and you may not be able to access the host). Be sure to add all the ports that are required before proceeding.

---

- Step 9** In the **UDP Ports** area, click **Permit Only** and click **Add**.
- Step 10** Type the number of a port that you want to enable on this host, and click **Add**.



#### Note

Disabling UDP port 137 impacts Microsoft NetBIOS naming. If you disable this port you will not be able to resolve the host name if you try to contact it on a Windows network. You can, however, still contact the host using its IP address.

---

- Step 11** Repeat steps 8–9 until you have added all the UDP ports you wish to enable.



#### Note

If you leave the UDP list blank, **all** port connections of that type are disabled. Be sure to add all the ports that are required before proceeding.

---

- Step 12** When finished adding ports, click **OK** until you are returned to the desktop.
- Step 13** When prompted, restart the host.
- Step 14** Test the functionality of the Niagara software and other applications (RCMD, NetMeeting) to verify that you can still access them on the host.
-

# Using a Virtual Private Network

An alternate method of securely connecting Internet-attached Niagara hosts is through the use of a virtual private network (VPN).

A VPN is an encrypted IP connection between hosts over a public infrastructure such as the Internet or the public telephone network. A VPN embeds a special protocol within the TCP/IP packets carried over the Internet. This concept of a second network protocol within a primary protocol is called tunneling. The following tunneling protocols are commonly found in VPN installations:

- PPTP (point-to-point tunneling protocol)
- IPSec (IP security protocol)
- L2TP (layer 2 tunneling protocol)

Along with encryption, many VPNs also include strong authentication of remote users or hosts and ways to hide information about the private LAN from hosts on the public network. A VPN can be between an individual computer and a LAN or can be LAN-to-LAN. Many companies use a VPN for connecting traveling or teleworking users, or for connecting small, remote sites to the corporate LAN.

Typically, a VPN architecture is comprised of:

- a client running software that is configured with parameters such as server IP address and tunneling protocol. The client could be an individual workstation (for computer-to-LAN VPNs), or another router or server (for LAN-to-LAN VPNs).
- a server device that handles the client connection, authentication, and decryption of the information from the client. A VPN server could be part of a firewall, or be a separate device.

Some advantages of using VPNs include:

- the client actually becomes part of the remote LAN (it receives an IP address on the remote LAN) and therefore has access to any resources on the LAN.
- cost can be lower than direct-dial (no extra telephone lines, RAS equipment to maintain, or long distance charges).
- if using cable or DSL connection, transmission speed can be faster than using direct-dial.

Some disadvantages include:

- overhead makes any VPN connection slower than a native (no VPN) dial-up or cable/DSL connection.
- host will not connect if the Internet connection to the ISP or from the ISP to primary site is down.

## Niagara System Architectures

Figure 6-13 on page 6-25 provides examples of typical Niagara job configurations (system architectures) for connecting Niagara hosts with a VPN. This drawing is similar to those used in previous architecture discussions, but several sites at fictional ABC company have been removed for simplicity.

Company ABC has implemented VPN server software on their firewall, and added a new site (site 7). The router in site 7 has VPN client software, which has been configured to provide a persistent VPN connection to the firewall in site 1. After the router connects to the Internet, the client software connects to the VPN at site 1, receiving new network settings as defined by the VPN server. The router (and by extension, the JACE-NP) are now part of the LAN.

The company has also loaded and configured client software on the remote engineering station to allow the off-site SI to maintain Niagara stations and hosts. Formerly, this maintenance was handled through dial-up to the JACE-NP in site 1 (see Figure 4-2).

The engineering station connects to the Internet through its ISP, then initiates the VPN client. The client connects to the company firewall and the engineering host receives an IP address belonging to ABC company, joining its network. Until the remote host disconnects the client software, all packets from the engineering host are routed onto the ABC company's network. The firewall has been configured to allow the remote engineering station access only to the Niagara hosts available on the company network, including those in sites 1, 2, and 7.

## Things to Note

You should note the following things about using Niagara hosts with a VPN:

- You cannot use a VPN with a JACE-4/5 connected directly to an ISP. That is because you cannot load VPN client software on a JACE-4/5. You can use a JACE-4/5 with a VPN if the JACE connects to the Internet through an on-site router that provides VPN services (as well as DHCP and NAT). This is similar to the setup shown in site 7.
- You may be able to load VPN client software on a JACE-NP, if the software can be configured to start automatically after connection by RAS to the ISP. For more information about connecting a JACE-NP to an ISP with RAS, see “Connecting Windows-based Hosts via Telephone Modem,” page 5-26.



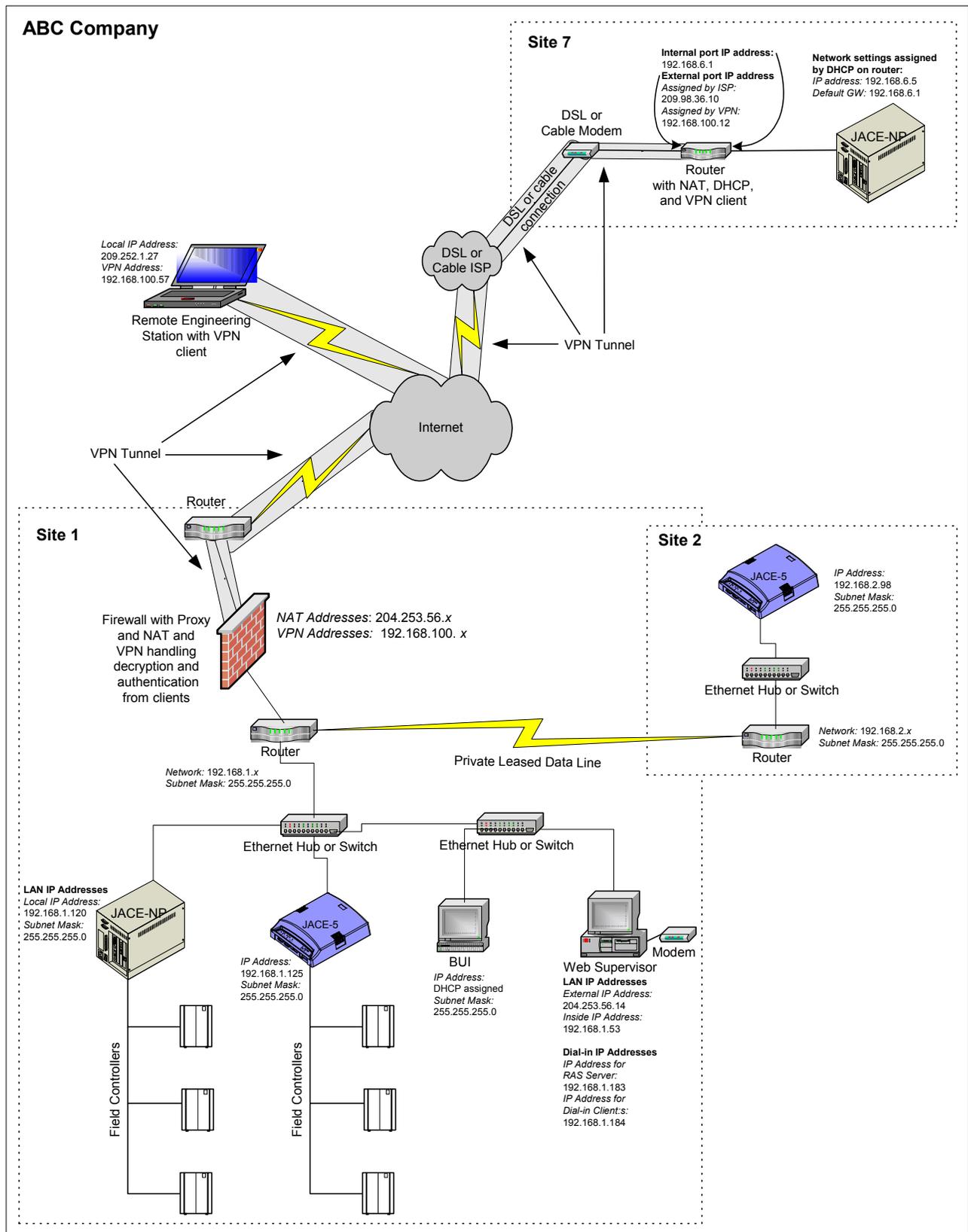

---

**Note** This scenario has not been tested by Systems Engineering. We recommend that you set up a pilot to test them before implementing in a live job.

---

- Exact details on how to connect Niagara hosts using VPNs cannot be provided due the many differences in VPN connection devices.

Figure 6-13 VPN in use at ABC Company.





## Configuration Files Used for Communication

This section provides a summary and some additional information about files used for communication functions by Niagara host. It uses the following conventions:

- **%SystemRoot%**—the directory where Windows is installed. Typically, this is `c:\winnt`. **%SystemRoot%** is a Microsoft convention you may also see used in Windows environment variables and path statements.
- **<release>**—Niagara release version.
  - On Windows-based hosts, this could be one of a number of release subdirectories of `<x>:\niagara\` where `<x>:\` is the hard drive that Niagara is installed on, typically `D:\`.
  - On VxWorks hosts, this is the current release directory. For information on determining the current release directory, see “[Determining the Current Release Directory](#),” page 6-12.
- **<stationname>**—the name of any station stored or running on the host.
  - On Windows-based hosts, this could be one of a number of stations.
  - On VxWorks hosts, this is the currently running station.

## Windows-based Niagara Hosts

[Table A-1](#) lists files used in communications on Windows-based Niagara hosts. This section uses

**Table A-1** Communication files used on Windows-based Niagara hosts.

| File               | Location                                                  | Purpose                                                                                                                                                                                                                                                                              |
|--------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hosts              | <code>%SystemRoot%\system32\drivers\etc</code>            | A file with a manually built list used to resolve an IP address to a name. You can edit this file using the <b>Admin Tool</b> . Click the <b>Network Settings</b> tab and click <b>Edit Hosts File</b> . See also “ <a href="#">The HOSTS File</a> ,” page 1-26.                     |
| station.properties | <code>&lt;release&gt;\stations\&lt;stationname&gt;</code> | Used to control configuration of the station, including whether the station auto starts. Also used to change the httpPort used by the Admin Tool for station functions. See also “ <a href="#">Changing the HTTP Port used by the Admin Tool for Station Functions</a> ,” page 6-11. |

JACE-4/5

**Table A-1** Communication files used on Windows-based Niagara hosts.

| File                | Location           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| drivers.properties  | <release>\nre\lib\ | Used to implement and configure various drivers. You can edit this file using the <b>Admin Tool (Installation tab)</b> . Typically you do not need to edit this file unless configuring a specific driver (follow instructions in the integration document). Parameters of special note used in communications on this platform: <ul style="list-style-type: none"> <li>• <b>comm.driverClass</b>—provides access to the serial ports. The driverClass property is platform specific and must be present. You should never modify it.</li> </ul> |
| system.properties   |                    | Used to configure properties of the system (host). For this platform, you can only edit using a text editor (not through the Admin Tool). Parameters of special note used in communications on this platform: <ul style="list-style-type: none"> <li>• <b>resolveIPAddresses</b>—when true, indicates whether the system should resolve IP addresses of incoming communications to host names before allowing connection. Default is false.</li> </ul>                                                                                           |
| niagarad.properties |                    | Used to configure niagarad, the Admin Tool interface to the OS. Also used to change the default port you use to connect to the host with the Admin Tool. Must be edited with a text editor (not through the Admin Tool). See also <a href="#">“Changing the Administration Port (3011),”</a> page 6-12.                                                                                                                                                                                                                                          |
| ddns.properties     |                    | Used to configure properties of the TZO DDNS service. Typically not used on this platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ipchanges.txt       | <release>\nre\user | Lists any IP address change that you make with the Admin Tool. See <a href="#">“About the ipchanges.txt file,”</a> page 3-16.                                                                                                                                                                                                                                                                                                                                                                                                                    |

## JACE-4/5

[Table A-1](#) lists files used in communications on VxWorks-based Niagara hosts.

**Table A-2** Communication files used on JACE-4/5s.

| File               | Location                                       | Purpose                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| station.properties | <release>\stations\ <i>&lt;stationname&gt;</i> | Used to control configuration of the station, including whether the station auto starts. Also used to change the httpPort used by the Admin Tool for station functions. See also <a href="#">“Changing the HTTP Port used by the Admin Tool for Station Functions,”</a> page 6-11.                                                               |
| system.properties  | \sys                                           | Used to configure properties of the system (host), including enabling telnet and FTP servers. For this platform, you can edit it using the Admin Tool ( <b>Host &gt; Edit System Properties</b> ). See also <a href="#">“Telnet,”</a> page 2-14 and <a href="#">“FTP,”</a> page 2-17.                                                            |
| port.properties    |                                                | Used to configure the serial ports of a JACE-4 only. See <a href="#">“Enabling the JACE-4 Modem (Internal or External),”</a> page 4-10.                                                                                                                                                                                                          |
| event.log          |                                                | The file associated with the Event Log function of the Admin Tool ( <b>Host &gt; View Event Log</b> ), which is used only on this platform. The niagara daemon reports troubleshooting information here. See <a href="#">“Troubleshooting Connection Problems,”</a> page 5-19 and <a href="#">“Troubleshooting DDNS Connections,”</a> page 5-24. |

Table A-2 Communication files used on JACE-4/5s.

| File                | Location           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hosts               | \sys\net           | A file with a manually built list used to resolve an IP address to a name. You can edit this file using the <b>Admin Tool</b> . Click the <b>Network Settings</b> tab and click <b>Edit Hosts File</b> . See also “ <a href="#">The HOSTS File</a> ,” page 1-26.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ras.properties      |                    | Used to both configure modems and enable the direct dial function. See “ <a href="#">About the ras.properties File</a> ,” page 4-12.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ddns.properties     |                    | Used to configure properties of the TZO DDNS service. See “ <a href="#">About the ddns.properties file</a> ,” page 5-23.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| net.properties      |                    | Contains DNS configuration properties (this platform only) as set with the Admin Tool ( <b>Network Settings</b> tab). Parameters of special note used in communications: <ul style="list-style-type: none"> <li>• <b>domainName</b>—DNS domain in which the JACE resides</li> <li>• <b>dnsServerList</b>—list of DNS server IP addresses</li> <li>• <b>defaultGateway</b>—IP address of default gateway</li> </ul>                                                                                                                                                                                                                                                                                  |
| drivers.properties  | <release>\nre\lib\ | Used to implement and configure various drivers. You can edit this file using the <b>Admin Tool</b> ( <b>Installation</b> tab). Typically you do not need to edit this file unless configuring a specific driver (follow instructions in the integration document). Parameters of special note used in communications on this platform: <ul style="list-style-type: none"> <li>• <b>comm.driverClass</b>—provides access to the serial ports. The driverClass property is platform specific and must be present. You should never modify it.</li> <li>• <b>comm.enumPorts</b>—when set to true will list available serial ports in the Standard Output window of the station on startup.</li> </ul> |
| niagarad.properties |                    | Used to configure niagarad, the Admin Tool interface to the OS.† Also used to change the default port you use to connect to the host with the Admin Tool. Must be edited with a text editor (not through the Admin Tool). See also “ <a href="#">Changing the Administration Port (3011)</a> ,” page 6-12.                                                                                                                                                                                                                                                                                                                                                                                          |





A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

# Commonly Used Terms

---

## A

**Active Directory**

Active Directory is the Microsoft Windows 2000 server directory service. It identifies resources on the network and makes those resources available to applications and users. In previous versions of Windows server, this function was handled by a combination of DNS, WINS, and the proprietary Windows domain function.

**Admin Tool or administration tool**

The Admin Tool is installed with the Java Desktop Environment (JDE) during the Niagara Web Supervisor software installation. You use Admin Tool to configure host-level functions (network settings, OS upgrades, station installations, etc.) on Niagara hosts.

**application proxy**

One of the security techniques commonly used on a firewall. This technique inserts a true barrier between the client computer, which is requesting access to an application, and the application server. The client actually connects to the application proxy, which acts on behalf of the client, negotiating with the destination application server for information.

**AT command set**

Industry-standard command language used to communicate with the modem. A modem could support the standard or extended AT command set. The AT prefix tells the modem that one or more commands follow. Settings made via AT commands are automatically reused by the modem until another command is received to change them, or the modem is turned off.

## B

**backbone**

A backbone is the main cable in a network through which data passes. It can also be used to mean the collection of major pieces that make up an individual network (such as the cable and the routers).

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>browser</b>                      | A browser is sometimes also called a Web browser. This is an application such as Microsoft Internet Explorer or Netscape Communicator, widely used to locate and display pages on the World Wide Web.                                                                                                                                                                                                                                                  |
| <b>BUI</b>                          | Browser User Interface. An acronym sometimes used to mean the user access of a Niagara station (JACE controller or Web Supervisor) using a Web browser, as opposed to using Java Desktop Environment (JDE).                                                                                                                                                                                                                                            |
| <b>C</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>category 5 cable</b>             | The most common type of twisted-pair cable found in LANs. A category 5 cable can operate at speeds of up to 100 Mbps.                                                                                                                                                                                                                                                                                                                                  |
| <b>class</b>                        | See <a href="#">IP address class</a> .                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>client</b>                       | An application on a computer (or other device) making a request of a <a href="#">server</a> device. For instance, a Niagara host can be a DHCP client, requesting networking setup information from a DHCP server.                                                                                                                                                                                                                                     |
| <b>click</b>                        | To click is to tap a mouse button, pressing it down and then immediately releasing it. Clicking a mouse button is different from pressing (or dragging) a mouse button, which implies that you hold the button down without releasing it. When used in an instruction, click means to move the mouse pointer over the object and click the left mouse button (sometimes called button number one). See double-click and right click for related terms. |
| <b>command line</b>                 | An area on the display screen provided by the operating system for the typing of commands. It is the line that shows the most recently displayed command prompt.                                                                                                                                                                                                                                                                                       |
| <b>command-line interpreter</b>     | The part of the operating system that processes what you type at a command line.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>command prompt</b>               | The area on the display screen that points to the command line.                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Console or Console window</b>    | The console is a command line window that allows command-line Niagara applications to be run.                                                                                                                                                                                                                                                                                                                                                          |
| <b>context or context-sensitive</b> | A program feature that causes a displayed element to change depending on the current selection or operation. For instance, context-sensitive help provides documentation for the specific object that you have selected. That object is referred to as the context.                                                                                                                                                                                    |

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

**crossover cable** A crossover cable can be used to connect two computers together without a hub, or to connect two hubs together (if the hub does not have an uplink port). If your hub has an uplink port, then you should use a standard Ethernet patch cable to connect the hubs instead.

**D**

**daemon** Typically, a process that performs administrative tasks for the operating system. It runs in the background and performs tasks at predefined times or in response to certain events.

In the Niagara environment, the Niagara daemon is an interface from the Admin Tool to the operating system. On the JACE-4/5 it also manages dial connections for captive ISP. On a Windows-based Niagara host, the Niagara service (which runs the niagarad.exe program) performs the daemon function; on a JACE-4/5 this is performed by the niagarad.exe program.

**default gateway** The IP address of a router used for communication with other networks. A host can communicate with any other host on its local subnet directly, but the default gateway defines the path to other hosts off the local subnet.

**dialog box** A graphical element (in the form of a box) used in Windows to display information or request input. Typically, dialog boxes request information and pop-ups convey information. They are both temporary—they disappear once you have entered the requested information and click OK.

**DDNS** Dynamic DNS (DDNS) is an Internet standard that specifies an automatic method for updating DNS records. DDNS can take one of two forms. It can be server-based service implemented within a company to update DNS records for hosts on the company LAN for local name resolution. It can also be service offered by some Internet companies to update the name-to-address mapping of Internet hosts that receive a dynamic IP address from their ISPs.

**DHCP** One of the techniques used to automatically assign network settings (such as IP address, subnet mask, default gateway, and DNS server) to a host.

**DNS** The domain name system (DNS) is the mechanism used by hosts to resolve names on the Internet, and on some private networks as well. Hosts that participate in the DNS system have names like “www.tridium.com”. Domain names must be globally unique so the data intended for that domain gets there and not to some other address. See also [fully qualified domain name](#).

**double-click** Some operations require a double-click, which means that you click the (left) mouse button twice in rapid succession.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

- domain name system** See [DNS](#).
- driver** A software program that acts as a translator between a computer and another device. Drivers are specific to each device, as they contain special commands for that device. Many devices require drivers, such as printers, hard drivers, modems and keyboards.
- dynamic DNS** See [DDNS](#).
- dynamic IP address** An IP address that is dynamically assigned to the host from a server. Typically, a dynamic address also changes with some frequency. Common technologies for dynamic assignment include DHCP and BootP. See [static IP address](#).

**E**

- engineering PC** Any PC in the Niagara environment that has the JDE loaded on it. This could be a Web Supervisor PC (which is used primarily as a server for Niagara integrations), or it could be a technician's PC, used strictly to maintain Niagara hosts.
- Ethernet** A popular LAN architecture based on the IEEE 802.3 networking standard. Networking standards describe how data is accessed and transferred over the physical media such as NICs and cabling.

**F**

- firewall** A firewall provides network security by restricting access to or from the network. A firewall can be a packaged unit sold as a complete firewall solution, or it could be a software package that is loaded on an existing computer situated such that it is the mediator between the network and the Internet.
- FQDN** See [fully qualified domain name](#).
- fully qualified domain name** A fully qualified domain name is composed of a host name, a domain name, and a top-level domain. For example, the FQDN *mail.bbs.uk* is a fully qualified domain name with *mail* being the host, *bbs* being the domain, and *uk* being the top level domain.

**G**

- Gx object** Graphics object, meaning any of the 11 types of Gx primitive objects you can add in a GxPage container to create a graphic viewable both in WorkPlace Pro and a Web browser. Gx object types include GxBarGraph, GxBoolean, GxDamper, GxFan, GxFloat, GxImage, GxInteger, GxPipe, GxSpectrum, GxText, and GxTimePlot.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z****H**

- host** A device on an IP network. This could be a PC, a router, a printer, or any other device that is configured with at least one IP address.
- HOSTS file** The HOSTS file is a text file residing on each local machine. Each line of the text file typically contains an IP address of a host and a name for it. HOSTS files were the original mechanism used to resolve an IP address to a name, but now other technologies, such as WINS, DNS, and DDNS are more common.
- HTTP** Hypertext transfer protocol. The protocol used by the World Wide Web. HTTP defines how Web servers and browsers transmit and format messages, including actions commands. HTTP is called a stateless protocol because each command is executed independently, without knowledge of the commands that came before it. Newer technologies such as Java overcome this limitation to make Web pages react intelligently. The other main standard that controls how the World Wide Web works is HTML, which determines how Web pages are formatted and displayed.

**I**

- interstation links** Links between two Niagara stations for the purposes of passing real-time data. Also known as an external link, because the link is external to the station database. To create an interstation link, each station must have the other station in its address book, and the address book entries must have valid user names and passwords.
- IP** Internet protocol. See [TCP/IP](#) and [protocol](#).
- IP address** In IP version 4, an IP address is a 32-bit number which uniquely identifies a host on the Internet. It is typically written in dotted decimal form *nnn.nnn.nnn.nnn* (for example, 192.168.1.1 or 27.34.100.3). Like a telephone number that is used to direct a call to a company, an IP address is used to direct data to a computer (for example, displaying a web page with a browser).
- IP address class** An IP address is made up of two parts, the network portion and the host portion. The class determines which portion of the address belongs to the network and which part belongs to the host. There are five classes, A-E, but hosts are only assigned IP addresses from classes A-C.

**J**

- JACE or JACE controller** Java Application Control Engine (rhymes with “pace”). The Tridium-manufactured controller that runs the core runtime Niagara software in a Java Virtual Machine (JVM), providing a station with direct support for field device integration plus

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

enterprise LAN connectivity. Since a station database is made using Java objects, it can easily run on multiple platforms ranging from a network computer that supports embedded systems to a desktop server platform that integrates multiple systems.

**JACE-NP**

The JACE-NP is the first of the JACE controller platforms, essentially a compact PC platform with an integral hard drive, but no keyboard, mouse or monitor. It uses either Windows NT 4.0 Workstation or Embedded Windows NT 4.0 as its operating system. The JACE-NP is designed for panel mounting in mechanical room or factory floor applications.

**JACE-4/5**

Refers to a JACE-4 or JACE-5 series controller. Each uses the Wind River VxWorks operating system and features a compact embedded processor platform with flash memory for backup.

**JDE**

Java Desktop Environment. The graphical engineering tool for creating Niagara station databases (formerly WorkPlace Pro).

**Java applet**

A Java program designed to be run from within another application (cannot run standalone from the operating system). The Niagara WebUIService includes a number of Java applets accessible from a browser, for example, GxPage graphics, log charts, and schedule and calendar editors. These applets are “served up” by the various WebUIService servlets.

**JVM or Java virtual machine**

The Java virtual machine is a self-contained operating environment that behaves as if it were a separate computer. It acts as the bytecode interpreter and runtime environment for Java applets, which are not given any direct access to the host operating system. This design has two distinct advantages: system independence and security.

Java applications are platform independent because they run the same in any JVM regardless of the hardware and software underlying the system. In addition, because the JVM has no direct contact with the operating system, there is little possibility of a Java applet damaging other files or applications.

**K****L****LAN**

Local area network. A group of computing devices (such as PCs, servers, and printers) that are connected together in a fairly concentrated geographic area (such as a floor of a building or several buildings). See also [WAN](#).

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

- leased line** A leased line is a high-speed data line leased from a telecommunications carrier. It provides a point-to-point connection between geographically dispersed sites. Data on a leased line is private; it does not travel on a public network. Typically, they are used to connect offices of a company into a WAN, or to connect a company to the Internet. Also referred to as T-1 (max speed 1.544 Mbps) or T-3 (43 Mbps) lines.
- localhost** The friendly name for the IP address 127.0.0.1, which is the loopback address. The loopback address is the logical network used by the local machine to address itself. For instance, when connecting to a Niagara station running on your PC, you can open the station using the assigned IP address for the network, or the loopback address 127.0.0.1, or the name “localhost”.
- M**
- MAC address** Media access control address. A unique address assigned to each NIC used to pass data to and from the computing device.
- N**
- NAT** Network address translation. The use of private IP addresses is commonly teamed with a technique called Network Address Translation (NAT) to provide access to the Internet by hosts that require it. Typically, some device (such as a router, firewall, or proxy server) has a supply of legitimate addresses and translates between a private address and a public one for a host that needs access to or from the Internet.
- network architecture** A description of the design of the network. In this document, an architecture typically includes both a text description and an illustration of the primary hardware and software pieces that make up the network.
- network mask** The network mask is used to define the network portion of the IP address and indicate whether the network is subnetted. For example, 255.255.255.0 is the network mask for a class C network that has not been subnetted. The mask 255.255.192.0 is an example of a valid mask for a subnetted class B network. Each host on a TCP/IP network requires a subnet mask even on a single-segment network.
- Niagara daemon** See [daemon](#).
- Niagara Console** See [Console](#) or [Console window](#).
- NIC** Network interface card. These devices act as the physical interface or connection between the computing devices (such as a printer or computer) and the network cable. NICs can be installed in an expansion slot in each computing device, or can be built onto the motherboard as is the case on a JACE-4/5.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

**null modem cable** A null modem cable is like a modem cable but is specially designed to hook two computers together, rather than a computer and a modem. The cable attaches to male serial (RS-232) ports on each computer.

**O**

**OS** Operating system. It is the base program installed on a computer. It is used to run other programs, and is responsible for basic functions of the computer such as accepting keyboard input, keeping track of files on the hard disk, and controlling peripheral devices.

**P**

**packet** In IP networks, a packet contains a small bit of data along with information about the source and destination IP addresses of the hosts sending and receiving the data. Typically, many packets make up the complete data transmission from one host to another. Packets are also known as datagrams.

**patch cable** An Ethernet cable used to connect a host and a hub.

**platform** Refers to the underlying hardware or software of a system. In this document, it is most often used to differentiate between the models of controllers based on operating system (the JACE-4/5 platform versus the JACE-NP platform). In some instances, it is used to differentiate between two models within the OS group (Embedded NT platform versus the Full NT platform).

**port** In TCP/IP networking, ports are used for long term conversations between two hosts (such as a client accessing a web page on a server). A port is a communication channel that allows different applications (such as FTP, HTTP, and SMTP) on the same computer to use network resources without interfering with each other.

**private IP address** A range of IP numbers set aside by the designers of the Internet for use in private networks. They allow organizations to implement IP addressing without having to apply to an ISP for unique global (public) IP addresses for every host. Hosts using these private addresses cannot be reached directly from the Internet (nor can they communicate to the Internet). See also [public IP address](#).

**protocol** A set of standards that define how computers (or processes) talk to one another. In order for the computers to talk, both must implement the same protocol.

**proxy server** A device usually implemented to provide connection sharing at a company. This means the company can have fewer public IP addresses used by many more hosts with private IP addresses. See also [application proxy](#).

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

**public IP address** An IP address that is in the public address space. It can be reached directly from the Internet, without the use of [NAT](#). See also [private IP address](#).

**Q****R**

**right-click** Some operations require that you click the right mouse button (sometimes called button two). Even though a mouse can be programmed to switch buttons, by convention 'clicking' refers to the left mouse button. In this guide, the term right-click is used anywhere you need to use the right mouse button.

**router** A device used to connect otherwise independent wiring segments, sub-networks, or complete LANs. Routers extract data from the [packet](#) and use [protocol](#) information in the packet to move data through the network along the most expedient route to its destination. Routers also divide networks logically instead of physically—an IP router can divide a network up into separate subnets so that only traffic destined for particular IP addresses can pass between segments.

**S**

**server** Typically, a computer on a network that returns data requested of it by other computers (the [clients](#)). It can also manage other network resources. Examples of types of servers include: file servers (stores files from users); DNS servers (manages name resolution); network servers (manages network resources); Web server (hosts Web pages). Servers can be dedicated to a single function or serve multiple ones.

**servlet** A servlet is a Java application that serves up Java applets. See [Java applet](#).

**service** In generic computing terms, a service is an application that does some work on or for a server. For instance, a database service stores and retrieves data in a database. Some Niagara services are located in the services container of the station (such as the LogService), but others operate at the system level (such as the remote access service). See also [daemon](#).

**SMTP** Simple mail transfer protocol. The protocol used by Internet mail servers to transfer mail to each other. Typically, server port 25 is the standard port used for SMTP.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

- static IP address** An IP address that is manually assigned to a host, and rarely changes. Typically, when the IP address is statically assigned, other network settings (such as [network mask](#) and [default gateway](#)) are also statically assigned. See [dynamic IP address](#).
- Standard Output window** An Admin Tool option providing a special window to view and save a running station's activity. Standard Output displays JVM station requests and responses in real time, including station startup messages. It is typically used for troubleshooting.
- stateful inspection** This firewall security technique is also known as “dynamic packet filtering”. It tracks a transaction in order to verify that the destination of an inbound packet matches the source of a previous outbound request. In doing so, it opens the packet and examines it for legitimacy.
- station** The JVM that hosts the running of objects, plus a station database containing all object configuration. Provides the environment to configure, manage, and run a single database of objects and the services required to support a control application.
- subnet mask** See network mask.
- supervisor or supervisor station** You can organize Niagara stations into hierarchies by defining a Niagara station to be the peer, subordinate, or supervisor of other stations. Relationships can provide convenience in configuring and managing stations. For instance, you can choose to “Backup Subordinates” and all stations defined as subordinate to the issuing station will be backed up.

**T**

- TCP/IP** Transmission Control Protocol/Internet Protocol is the suite of communications protocols used to connect hosts on the Internet. The two main protocols included are TCP and IP. TCP/IP originated with UNIX, but now most operating systems support TCP/IP as a networking standard.
- terminal emulation** A program to access a server as if you were sitting at the server console.
- time synchronization** With time synchronization, one host can receive updates to its system time from another host. A Niagara host can function as both a time synchronization client and a time synchronization server. Niagara hosts can also use Internet time synchronization servers for system time updates.
- tree view** The portion of the WorkPlace Pro window that shows the hierarchical structure of the station database. Tree view operates much like Windows Explorer, where you expand container (parent) nodes to see subordinate child nodes.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z****U**

**URL** Uniform resource locator. The global address of a document or other resource. Within the context of Niagara, a URL is similar to a SWID. A SWID defines a particular node in a Niagara station database, whereas a URL can include a SWID or a resource located elsewhere.

**V**

**VxWorks** A real-time operating system for embedded devices by WindRiver Systems. This is the OS for the JACE-4/5 [platform](#).

**W**

**WAN** Wide area network. A group of [LANs](#) connected with telephone or data lines to form one network.

**Web Supervisor** Refers to a Niagara station running on a PC, which is typically configured as the supervisor station for any networked JACE controller(s). Typically, this PC is also running the full suite of Niagara applications, including Java Desktop Environment and the Alarm Console.

**WebUIService** Web user interface service. This service is required by a Niagara station to provide a set of views to its objects when using a Web browser connection. The WebUIService is a suite of [servlets](#) that use HTML and [Java applets](#) to provide a browser user interface ([BUI](#)). Servlets included are the GxServlet, ChartServlet, ScheduleServlet, StatusServlet, AlarmServlet, and TextServlet.

**WINS** The Windows Internet naming service is Microsoft's Windows-only name resolution protocol. Like [DNS](#), WINS is also implemented with a series of servers that maintain databases of host names to IP addresses. However, setting up WINS is easier than setting up a DNS because WINS actually receives most address records automatically from the WINS clients.

**wizard** A utility within an application that helps you use the application to perform a particular task. For instance, the New Station wizard guides you through the configuration of a station node, which makes the process of adding a new station very simple.

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z****X****XML**

eXtensible Markup Language. A specification developed by the W3C (World Wide Web Consortium). XML is a subset of SGML, designed especially for Web documents. Use of custom tags provides “extensibility”, not available using HTML. XML is expected to eventually supplant HTML as the standard for Web documents. The Niagara Framework uses XML as one method of station database storage.

**Y****Z**

**A**

access methods

- contention methods [1-13](#)
- overview [1-13 to 1-14](#)
- polling [1-14](#)
- token passing [1-13](#)

account

- Administrator [3-5](#)
- Guest [3-5, 3-6](#)

Active Directory [3-6](#)

adapters, serial and null modem

- about [2-12](#)
- JACE-4 [2-12, 4-12](#)
- JACE-5 [2-12, 4-11](#)

Add Address button [4-32](#)

Add RAS Device dialog box [4-21, 4-28](#)

address book [5-5](#)

address book, station [4-6, 4-32, 5-5, 5-6, 5-8, 6-19](#)

administrator passwords, caution about changing [6-2](#)

Administrators group [3-6](#)

Advanced button [3-9](#)

alarm archiving [1-35, 6-8](#)

Alarm Console acknowledgement [1-36, 4-2, 4-32, 5-2, 6-8](#)

alarming, Niagara [1-35, 6-8](#)

alarms [5-2](#)

Allowed Users dialog box [4-30](#)

applets [6-5](#)

architectures

- direct dial
  - design considerations [4-5 to 4-7](#)
  - discussion [4-2 to 4-3](#)
- ISP
  - cable or DSL modem [5-4](#)
  - design considerations [5-6](#)
  - NAT and DSL/cable [5-4](#)
  - telephone modem

JACE-4/5 [5-2 to 5-3](#)

Windows hosts [5-3](#)

## LAN

discussion [3-1 to 3-3](#)

things to note [3-4](#)

VPN [6-24](#)

## WAN

discussion [3-3](#)

things to note [3-4](#)

archive\_remote [1-35, 6-8](#)

archives [5-2](#)

archiving [1-35, 6-8](#)

arp command [3-24](#)

AT command set, about [4-9](#)

**B**

backup subordinate [1-36, 6-8](#)

baudrate [4-14, 5-11](#)

bindings, protocol [1-13](#)

bridges [1-15](#)

broadcast address [1-22, 3-19](#)

routers [1-16](#)

## button

Add Address [4-32](#)

Advanced [3-9](#)

Disconnect [2-11](#)

End Call [2-5](#)

Logoff [2-5](#)

Place Call [2-3](#)

Port Properties [4-10](#)

**C**

cable modem

- connecting hosts [5-27](#)
- connecting hosts discussion [5-4](#)
- cables
  - about Ethernet [3-10 to 3-12](#)
  - coaxial [1-7](#)
  - connectors [1-9](#)
  - crossover connection [3-14](#)
  - Ethernet pinouts [3-12](#)
  - fiber optic [1-8](#)
  - serial and null modem
    - about [2-12](#)
    - JACE-4 [2-12, 4-12](#)
    - JACE-5 [2-12, 4-11](#)
  - twisted pair [1-7](#)
- cabling, overview [1-7](#)
- captive ISP
  - about [5-8](#)
  - configuring, JACE-4/5 [5-8 to 5-21](#)
  - network settings [5-9 to 5-10](#)
- coaxial cable [1-7](#)
- command prompt, opening [2-20](#)
- command-line interpreter [2-8](#)
- command-line utilities, Windows [2-20](#)
- commands
  - arp [3-24](#)
  - dhcpcParamsShow(pDhpcBootCookie) [3-28](#)
  - dhcpcServerShow(pDhpcBootCookie) [3-27](#)
  - FTP [2-18, 2-19](#)
  - ifShow [3-27](#)
  - ipconfig [3-31](#)
  - net use [2-6](#)
  - netstat [2-25](#)
  - nslookup [2-23](#)
  - ping [2-21](#)
  - rcmd [2-6](#)
  - target shell [3-27 to 3-29](#)
  - telnet [2-15](#)
  - tracert [2-22](#)
- communication, Niagara hosts summary [1-35](#)
- Conn Properties dialog box [2-9](#)
- Config tab [6-10](#)
- configuration files, communication [A-1 to A-3](#)
- configuration, tools [2-1 to 2-19](#)
- Configure Modules dialog box [5-18](#)
- Configure Port Usage dialog box [4-22](#)
- configuring
  - dial-out [4-32 to 4-34](#)
  - engineering PC
    - direct dial [4-25 to 4-31](#)
    - RAS [4-28 to 4-31](#)
  - ISP e-mail [5-19](#)
  - JACE-4
    - serial ports [4-10 to 4-11](#)
  - JACE-4/5
    - captive ISP [5-8 to 5-21](#)
    - DDNS [5-23 to 5-24](#)
    - DHCP [3-25](#)
    - direct dial [4-7 to 4-16](#)
    - RAS [4-14 to 4-16](#)
  - JACE-NP
    - direct dial [4-17 to 4-25](#)
    - RAS
      - direct dial [4-20 to 4-25](#)
      - ISP [5-26](#)
- Connect to dialog box [2-9, 2-16, 4-40](#)
- Connect to Host dialog box [2-2](#)
- connecting
  - DHCP
    - engineering PC [3-30](#)
    - JACE-4/5 [3-24 to 3-26](#)
    - JACE-NP [3-30](#)
  - direct dial
    - engineering PC [4-25](#)
    - JACE-4/5 [4-7 to 4-16](#)
    - JACE-NP [4-17 to 4-25](#)
    - multiple JACEs, discussion [4-6](#)
    - user-initiated [4-34 to 4-44](#)
  - ISP
    - about [5-5](#)
    - cable or DSL [5-27](#)
    - telephone modem
      - JACE-4/5 [5-8 to 5-21](#)
      - JACE-NP [5-26](#)
      - Web Supervisor [5-26](#)
    - Windows hosts, discussion [5-26](#)
  - JACE-4/5 serial port [2-7](#)
  - LAN
    - any JACE [3-9 to 3-14](#)
    - engineering PC [3-6 to 3-9](#)

- Connection Availability dialog box [4-39](#)
  - Connection Complete dialog box [4-40, 4-42](#)
  - Connection Description dialog box [2-9, 2-16](#)
  - connections, direct dial types [4-4](#)
  - connectors
    - cable, overview [1-9](#)
    - DB-9 [2-13](#)
    - mode [2-9](#)
    - RJ-45 [2-13](#)
  - contention methods, network [1-13](#)
  - creating strong passwords [6-3](#)
  - crossover cables
    - about [3-10 to 3-12](#)
    - LAN connection [3-14](#)
  - current release directory, determining [6-12](#)
- 
- ## D
- Database service [1-35, 6-8](#)
  - DBAdmin error [6-11](#)
  - DDNS
    - about provider [5-22](#)
    - JACE-4/5
      - configuration [5-22 to 5-26](#)
    - JACE4/5
      - support [3-23](#)
    - Niagara summary [1-34](#)
    - overview [1-28](#)
    - registering with TZO [5-22](#)
    - troubleshooting
      - connections [5-24](#)
      - update failures [5-25](#)
  - ddns.properties
    - about [5-23](#)
    - configuring [5-23](#)
  - default gateway, overview [1-24](#)
  - default ports, changing
    - Administration Port (3011)
      - discussion [6-12](#)
      - JACE-4/5 [6-15](#)
      - JACE-NP [6-14](#)
      - Web Supervisor [6-13](#)
    - HTTP Port (80)
      - discussion [6-9](#)
      - station [6-9 to 6-10](#)
      - used by Admin Tool [6-11](#)
    - impact [6-18 to 6-20](#)
    - overview [6-9](#)
    - time synchronization [6-17](#)
  - Details tab [4-42](#)
  - determining
    - current release directory [6-12](#)
    - JACE-4/5 MAC address [3-23](#)
    - new JACE default network settings [3-10](#)
  - device parameter [5-11](#)
  - DHCP
    - configuring
      - engineering PC [3-30](#)
      - JACE-4/5 [3-25](#)
      - JACE-NP [3-30](#)
    - lease renewal failure
      - JACE-4/5 [3-26](#)
      - JACE-NP [3-31](#)
    - Niagara considerations [3-23](#)
    - Niagara summary [1-33](#)
    - notes
      - JACE-4/5 [3-24 to 3-26](#)
      - Windows-based host [3-29](#)
    - reservation not working
      - JACE-4/5 [3-26](#)
      - JACE-NP [3-31](#)
  - dhcpcParamsShow(pDhcpcBootCookie) command [3-28](#)
  - dhcpcServerShow(pDhcpcBootCookie) command [3-27](#)
  - dial-in versus dial-out [4-3](#)
  - dialog box
    - Add RAS Device [4-21, 4-28](#)
    - Allowed Users [4-30](#)
    - Comn Properties [2-9](#)
    - Configure Modules [5-18](#)
    - Configure Port Usage [4-22](#)
    - Connect to [2-9, 2-16, 4-40](#)
    - Connect to Host [2-2](#)
    - Connection Availability [4-39](#)
    - Connection Complete [4-40, 4-42](#)
    - Connection Description [2-9, 2-16](#)
    - Incoming Connections [4-29](#)
    - Incoming TCP/IP Properties [4-31](#)

- Location Information [4-35](#)
  - Logon [2-2](#)
  - Network Configuration [4-22](#)
  - Networking Components [4-30](#)
  - New Address [4-32](#)
  - New Phonebook Entry [4-36](#)
  - Open [6-13](#)
  - Phone and Modem Options [4-27](#)
  - Phone Number to Dial [4-38](#)
  - PPP TCP/IP Settings [4-37](#)
  - RAS Server TCP/IP Configuration [4-23](#)
  - Remote Access Setup [4-20, 4-22](#)
  - Select Distribution Directory [5-18](#)
  - Services [4-24](#)
  - Unlock Workstation [2-4](#)
  - Virtual Private Network [4-30](#)
  - dialOutOnly parameter [5-10](#)
  - Dial-Up Networking Monitor [4-40, 4-42](#)
  - dial-up networking. See DUN
  - direct dial
    - caution about avoiding File > Open Dial up (Station) [4-34](#)
    - configuring
      - engineering PC [4-25 to 4-31](#)
      - interstation communication [4-32 to 4-34](#)
      - JACE-4/5 [4-7 to 4-16](#)
      - JACE-NP [4-17 to 4-25](#)
    - connecting multiple JACEs [4-6](#)
    - connection types [4-4](#)
    - enabling dial-in, all hosts [4-16](#)
    - functionality [4-3 to 4-5](#)
    - granting dial-in permissions
      - engineering PC [4-31](#)
      - JACE-4/5 [5-15](#)
      - JACE-NP [4-25](#)
    - system architectures [4-2 to 4-3](#)
    - user-initiated connection [4-34 to 4-44](#)
  - Directory, Active [3-6](#)
  - Disconnect button [2-11](#)
  - disconnects
    - about [5-8](#)
    - avoiding with ISP [5-21](#)
    - IspConnection object [5-15 to 5-18](#)
  - DNS
    - how it works from host [1-27](#)
    - name servers [1-27](#)
    - overview [1-27](#)
    - propagation [5-25](#)
    - troubleshooting tool [2-23 to 2-25](#)
  - domain name system. See DNS
  - domain, Windows [3-5, 3-6](#)
  - domainName parameter [5-23](#)
  - drivers
    - installing modem
      - engineering PC [4-26](#)
      - JACE-NP [4-17](#)
    - overview [1-11](#)
  - DSL modem
    - connecting hosts [5-27](#)
    - discussion [5-4](#)
  - DUN
    - accessing host or station [4-43](#)
    - creating connection
      - Windows 2000 [4-38 to 4-39](#)
      - Windows NT 4.0 [4-35 to 4-38](#)
    - establishing connection
      - Windows 2000 [4-41 to 4-43](#)
      - Windows NT 4.0 [4-39 to 4-41](#)
  - dynamic DNS. See DDNS
  - dynamic host configuration protocol. See DHCP
- 
- ## E
- e-mail
    - configuring ISP [5-19](#)
    - notification [1-35, 6-8](#)
  - email parameter [5-23](#)
  - Embedded Windows NT 4.0 [1-32, 3-5](#)
  - enabled parameter [5-23](#)
  - enabling
    - dial-in [4-16](#)
    - JACE-4 modem [4-10](#)
    - telnet on a JACE-4/5 [2-14](#)
  - End Call button [2-5](#)
  - engineering PC
    - configuration files [A-1](#)
    - configuring

- DHCP [3-30](#)
- direct dial [4-25 to 4-31](#)
- RAS [4-28 to 4-31](#)
- granting dial-in permissions [4-31](#)
- installing modem [4-26](#)
- installing modem driver [4-26](#)
- specific security guidelines [6-3](#)
- starting RAS service [4-31](#)
- supported modems [4-26](#)
- user-initiated connection [4-34 to 4-44](#)

error, DBAdmin [6-11](#)

Ethernet cables

- about [3-10 to 3-12](#)
- pinouts [3-12](#)

event log [5-19, 5-24](#)

external modem, installing

- engineering PC [4-26](#)
- JACE-4/5 [4-11 to 4-12](#)
- JACE-NP [4-17](#)

---

## F

fiber optic cable [1-8](#)

file transfer protocol. See FTP

files

- communication [A-1 to A-3](#)
- ddns.properties
  - about [5-23](#)
  - configuring [5-23](#)
- HOSTS [1-26](#)
- ipchanges.txt [3-16](#)
- niagarad.properties [6-12](#)
- port.properties [4-10](#)
- ras.properties [5-13](#)
  - about [4-12](#)
  - configuring
    - captive ISP [5-10 to 5-15](#)
    - direct dial [4-14 to 4-16](#)
  - station.properties [6-11](#)
  - system.properties [2-14, 2-17](#)
  - transfer [2-17](#)

firewall

- overview [1-29](#)

- using with Niagara [6-4 to 6-6](#)

FTP

- caution about security risk [2-17](#)
- caution about station inoperability [2-17](#)
- commands [2-18](#)
- discussion [2-17](#)
- enabling, JACE-4/5 [2-17](#)

FTP commands [2-19](#)

full duplex [2-12](#)

---

## G

gateways [1-16](#)

General tab [3-8](#)

global data passing [1-36, 6-8](#)

group

- Administrators [3-6](#)
- Guests [3-6](#)

Guest account [3-5, 3-6](#)

Guests group [3-6](#)

guidelines for security [6-2](#)

GxPage [3-3](#)

---

## H

hexadecimal, converting [3-20](#)

host names, associating IP addresses [1-26 to 1-28](#)

hosts

- Niagara summary [1-32](#)
- other access methods [3-21](#)

HOSTS file [1-26](#)

HTTP

- changing default Niagara port [6-9](#)
- JDE use [6-5](#)
- port forwarding [5-7](#)

HTTPS [1-31](#)

hubs, overview [1-6](#)

Hyperterminal

- connecting, JACE-4/5 [2-8](#)
- disconnecting [2-9](#)
- overview [2-7](#)
- telnet [2-16](#)

**I**

ICMP [2-20](#), [2-22](#)

IEEE 802 standards, overview [1-10](#)

ifShow command [3-27](#)

Incoming Connections dialog box [4-29](#)

Incoming TCP/IP Properties dialog box [4-31](#)

initFailLogOnly parameter [4-14](#), [5-11](#)

initialization string [4-7](#)

initString parameter [4-14](#), [5-11](#)

Installation tab [5-18](#)

installing modem driver

engineering PC [4-26](#)

JACE-NP [4-17](#)

Internet control message protocol. See ICMP

Internet protocol. See IP and TCP/IP

Internet service provider. See ISP

interpreter, command-line [2-8](#)

interstation links

example

LAN [3-2](#)

WAN [3-3](#)

support

direct dial [4-6](#)

ISP [5-6](#)

LAN [3-4](#)

WAN [3-4](#)

IP

classes [1-19](#)

overview [1-17 to 1-19](#)

routing [1-24](#)

IP Address tab [3-7](#), [6-22](#)

IP addresses

allocation [1-23 to 1-26](#)

assigning, JACE [3-12 to 3-14](#)

associating host names [1-26 to 1-28](#)

broadcast [1-22](#)

determining lost

general [3-16](#)

JACE-4/5 [3-19 to 3-21](#)

JACE-NP [3-17 to 3-19](#), [3-21](#)

localhost [1-22](#)

loopback [1-22](#)

multicasting [1-22](#)

overview [1-19](#)

private

LAN [3-1](#), [3-4](#)

numbers [1-23](#)

overview [1-23](#)

public

LAN [3-1](#), [3-2](#), [3-4](#)

Niagara summary [1-33](#)

security impacts [6-1](#)

special [1-22](#)

static and dynamic [1-25](#), [5-2](#)

troubleshooting tool [2-27 to 2-28](#)

ipchanges.txt, about [3-16](#)

ipconfig [2-27 to 2-28](#), [3-29](#), [3-31](#)

ISP

about connecting [5-5](#)

configuring e-mail [5-19](#)

connecting

cable or DSL modem [5-27](#)

telephone modem

JACE-NP [5-26](#)

Web Supervisor [5-26](#)

Windows, overview [5-26](#)

connecting hosts, discussion

cable or DSL [5-4](#)

NAT [5-4](#)

telephone modem

JACE-4/5 [5-2](#)

Windows [5-3](#)

disconnects

about [5-8](#)

avoiding [5-21](#)

information required [5-9](#)

Niagara considerations [5-1 to 5-7](#)

Niagara system architectures [5-2 to 5-5](#)

selecting [5-7](#)

troubleshooting connection problems [5-19 to 5-21](#)

isp module [5-15](#)

ispBackupNumber parameter [5-12](#)

IspConnection object

controlling disconnects [5-15 to 5-18](#)

examples [5-16](#)

ispDisconnectTimex parameter [5-12](#)

ispPassword parameter [5-12](#)

ispPrimaryNumber parameter [5-12](#)  
 ispRetryCount parameter [5-12](#)  
 ispRetryDelay parameter [5-12](#)  
 ispUsername parameter [5-12](#)

---

## J

JACE, connecting multiple to Web Supervisor [4-6](#)  
 JACE-4  
   configuring serial ports [4-10 to 4-11](#)  
   serial and null modem cables and adapters [2-12, 4-12](#)  
 JACE-4/5  
   configuration files [A-2](#)  
   configuring  
     captive ISP  
       network settings [5-9 to 5-10](#)  
       overview [5-8 to 5-21](#)  
     DDNS [5-23 to 5-24](#)  
     DHCP [3-25](#)  
     direct dial [4-7 to 4-16](#)  
     RAS [4-14 to 4-16](#)  
   determining MAC address [3-23](#)  
   DHCP  
     lease renewal failure [3-26](#)  
     reservation not working [3-26](#)  
     troubleshooting [3-26 to 3-29](#)  
   enabling  
     FTP [2-17](#)  
     JACE-4 modem [4-10](#)  
     telnet [2-14](#)  
   granting dial-in permissions [5-15](#)  
   installing and configuring modems  
     direct dial [4-7 to 4-12](#)  
     ISP [5-9](#)  
   specific security guidelines [6-3](#)  
   telnet connection [2-15](#)  
 JACE-5  
   serial and null modem cables and adapters [2-12, 4-11](#)  
 JACE-NP  
   additional open ports [6-20 to 6-22](#)  
   caution about adding internal modem [4-17](#)  
   configuration files [A-1](#)  
   configuring

DHCP [3-30](#)  
 direct dial, overview [4-17 to 4-25](#)  
 RAS  
   direct dial [4-20 to 4-25](#)  
   ISP [5-26](#)  
 DHCP  
   lease renewal failure [3-31](#)  
   reservation not working [3-31](#)  
   troubleshooting [3-30 to 3-33](#)  
 granting dial-in permissions [4-25](#)  
 installing  
   external modem [4-17](#)  
   modem driver [4-17](#)  
 remote control utilities [2-2 to 2-7](#)  
 specific security guidelines [6-3](#)  
 starting RAS service [4-24](#)  
 supported modems [4-17](#)  
 Java  
   applets [6-5](#)  
   servlets [6-5](#)  
 JDE [1-35, 6-7](#)

---

## K

key parameter [5-23](#)

---

## L

LAN  
   configuring DHCP  
     engineering PC [3-30](#)  
     JACE-4/5 [3-25](#)  
     JACE-NP [3-30](#)  
   connecting  
     JACE [3-9 to 3-14](#)  
     Windows 2000 host [3-8 to 3-9](#)  
     Windows NT 4.0 host [3-6 to 3-8](#)  
   crossover cable [3-14](#)  
   Niagara considerations [3-1 to 3-6](#)  
   Niagara system architectures [3-1 to 3-3](#)  
   overview [1-2](#)  
   private IP address [3-1, 3-4](#)

## Chapter

public IP address [3-1](#), [3-2](#), [3-4](#)  
 things to note [3-4](#)  
 lastConnectionAttempt parameter [5-16](#)  
 lastSuccessfulConnection parameter [5-16](#)  
 layer  
   application [1-17](#)  
   data link [1-18](#)  
   network [1-18](#)  
   physical [1-18](#)  
   presentation [1-18](#)  
   session [1-18](#)  
   transport [1-18](#)  
 layered architecture [1-9](#)  
 local area network. See LAN  
 localAddr parameter [5-11](#)  
 localhost [1-22](#)  
 Location Information dialog box [4-35](#)  
 Logoff button [2-5](#)  
 Logon dialog box [2-2](#)  
 loopback address [1-22](#)

---

**M**

MAC address  
   definition [1-8](#)  
   JACE-4/5 [3-23](#)  
 Mail service [1-35](#), [6-8](#)  
 menu, Target's Desktop [2-4](#)  
 Microsoft Windows NT 4.0, disabling open ports [6-22](#)  
 Microsoft Windows Server, Niagara compatibility [3-4](#)  
 mode connector [2-9](#)  
 modem commands, about [4-9](#)  
 modemDebug [4-14](#), [5-13](#)  
 modems  
   about pre-configured, JACE-4/5 [4-7](#)  
   enabling, JACE-4 [4-10](#)  
   initialization string [4-7](#)  
   installing driver  
     JACE-NP [4-17](#)  
     Windows 2000 [4-26](#)  
     Windows NT 4.0 [4-26](#)  
   installing external  
     engineering PC [4-26](#)

  JACE-4/5 [4-11 to 4-12](#)  
   JACE-NP [4-17](#)  
   supported  
     engineering PC [4-26](#)  
     JACE-4/5 [4-7](#)  
     JACE-NP [4-17](#)  
 Modems tab [4-26](#)  
 module, isp [5-15](#)  
 monitor, station [1-36](#), [6-8](#)  
 multicasting [1-22](#)

---

**N**

name servers [1-27](#)  
 NAT  
   LAN example [3-1](#)  
   overview [1-23](#)  
   WAN example [3-3](#)  
 net use command [2-6](#)  
 NetMeeting  
   caution about station inoperability [2-3](#)  
   ending [2-5](#)  
   overview [2-2](#)  
   starting [2-3](#)  
 netstat [2-25 to 2-26](#)  
 network  
   access methods  
     overview [1-13 to 1-14](#)  
     polling [1-14](#)  
     token passing [1-13](#)  
   cabling, overview [1-7](#)  
   contention methods [1-13](#)  
   design overview [1-3 to 1-9](#)  
   drivers overview [1-11](#)  
   expanding overview [1-14 to 1-16](#)  
   hubs overview [1-6](#)  
   information resources [1-36](#)  
   interface card. See NIC  
   masks overview [1-20](#)  
   settings  
     caution about typing correct information [3-13](#)  
     determining lost  
       general [3-16](#)

- JACE-4/5 [3-19 to 3-21](#)
- JACE-NP [3-17 to 3-19, 3-21](#)
- new JACE determination [3-10](#)
- troubleshooting tool [2-27 to 2-28](#)
- types
  - peer-to-peer [1-3](#)
  - server-based, overview [1-3](#)
  - specialized servers, overview [1-3](#)
- use overview [1-2](#)
- wireless [1-8](#)
- network address translation. See NAT
- Network Configuration dialog box [4-22](#)
- Network Settings tab [2-2, 3-13, 3-25, 4-10, 4-14, 5-9, 5-13](#)
- Network tab [5-23](#)
- networking
  - concept [1-2](#)
  - introduction [1-1 to 1-16](#)
  - IP overview [1-16 to 1-32](#)
  - technologies, Niagara summary [1-33](#)
- Networking Components dialog box [4-30](#)
- New Address dialog box [4-32](#)
- New Phonebook Entry dialog box [4-36](#)
- Niagara architectures
  - direct dial [4-2 to 4-3](#)
  - ISP [5-2 to 5-5](#)
  - LAN [3-1 to 3-3](#)
  - VPN [6-24](#)
  - WAN [3-3](#)
- Niagara considerations
  - DHCP [3-23](#)
  - direct dial [4-1 to 4-7](#)
  - ISP [5-1 to 5-7](#)
  - LAN [3-1 to 3-6](#)
  - security [6-1 to 6-4](#)
  - summary [1-32 to 1-36](#)
- Niagara Console [2-6](#)
- Niagara hosts, summary [1-32](#)
- Niagara Remote Installation window [5-18](#)
- niagarad.properties
  - caution about editing [6-13](#)
  - editing [6-12](#)
- NIC, overview [1-8](#)
- Notepad [6-14](#)
- nslookup [2-23 to 2-25](#)

- null modem cables and adapters [2-12](#)

---

## O

- object, IspConnection [5-15 to 5-18](#)
- Open dialog box [6-13](#)
- open ports
  - additional JACE-NP [6-20 to 6-22](#)
  - disabling [6-22](#)
- open system interconnection. See OSI
- opening command prompt [2-20](#)
- OSI model
  - application layer [1-17](#)
  - data link layer [1-18](#)
  - layered architecture [1-9](#)
  - network layer [1-18](#)
  - overview [1-9](#)
  - physical layer [1-18](#)
  - presentation layer [1-18](#)
  - session layer [1-18](#)
  - transport layer [1-18](#)
  - with TCP/IP [1-17](#)

---

## P

- packet sniffer [3-18](#)
- packet, definition [1-12](#)
- parameters
  - baudrate [4-14, 5-11](#)
  - device [5-11](#)
  - dialOutOnly [5-10](#)
  - domainName [5-23](#)
  - email [5-23](#)
  - enabled [5-23](#)
  - initFailLogOnly [4-14](#)
  - initString [4-14, 5-11](#)
  - ispBackupNumber [5-12](#)
  - ispDisconnectTimex [5-12](#)
  - ispPassword [5-12](#)
  - ispPrimaryNumber [5-12](#)
  - ispRetryCount [5-12](#)
  - ispRetryDelay [5-12](#)

- ispUsername [5-12](#)
  - key [5-23](#)
  - lastConnectionAttempt [5-16](#)
  - lastSuccessfulConnection [5-16](#)
  - localAddr [5-11](#)
  - modemDebug [4-14](#), [5-13](#)
  - pppDebug [4-14](#), [5-13](#)
  - rasDebug [4-14](#), [5-13](#)
  - rasEnable [5-10](#)
  - rasMode [5-10](#)
  - rate [5-16](#)
  - remoteAddr [5-11](#)
  - serverx [5-23](#)
  - state [5-16](#)
  - statusOutput [5-16](#)
  - updateNvRamCmd [4-14](#), [5-11](#)
  - updateNvRamFlag [4-14](#), [5-11](#)
  - passwords
    - caution about changing administrator [6-2](#)
    - creating strong [6-3](#)
  - patch cable [1-5](#), [3-10](#)
  - peer-to-peer networks [1-3](#)
  - permissions, granting dial-in
    - engineering PC [4-31](#)
    - JACE-4/5 [5-15](#)
    - JACE-NP [4-25](#)
  - Phone and Modem Options dialog box [4-27](#)
  - Phone Number to Dial dialog box [4-38](#)
  - ping [2-20 to 2-22](#)
  - Place Call button [2-3](#)
  - Poll Archive service [1-35](#), [6-8](#)
  - polled archiving [1-35](#), [4-2](#), [6-8](#)
  - polling, overview [1-14](#)
  - Port Properties button [4-10](#)
  - port.properties file [4-10](#)
  - ports
    - about [1-31](#)
    - caution about disabling ports [6-22](#)
    - changing Niagara defaults [6-9](#)
      - Administration Port (3011)
        - discussion [6-12](#)
        - JACE-4/5 [6-15](#)
        - JACE-NP [6-14](#)
        - Web Supervisor [6-13](#)
      - HTTP Port (80) [6-9 to 6-10](#)
        - station [6-9](#)
        - used by Admin Tool [6-11](#)
      - impact [6-18 to 6-20](#)
      - time synchronization [6-17](#)
    - COM1, caution about communication interruption [2-8](#)
    - default Niagara numbers [6-7 to 6-8](#)
    - disabling open [6-22](#)
    - JACE-NP additional open [6-20 to 6-22](#)
    - troubleshooting [2-25 to 2-26](#)
  - PPP TCP/IP Settings dialog box [4-37](#)
  - pppDebug parameter [4-14](#), [5-13](#)
  - pre-configured modems, about [4-7](#)
  - private IP addresses
    - LAN [3-1](#), [3-4](#)
    - numbers [1-23](#)
    - overview [1-23](#)
  - protocols
    - bindings [1-13](#)
    - how they work [1-12](#)
    - OSI [1-12](#)
    - overview [1-11](#)
    - RS-232C [2-12](#)
    - stacks [1-12](#)
    - tunneling [6-23](#)
  - Protocols tab [3-7](#), [6-22](#)
  - proxy server
    - overview [1-28](#)
    - using with Niagara [6-4 to 6-6](#)
  - public IP addresses
    - LAN [3-1](#), [3-2](#), [3-4](#)
    - Niagara summary [1-33](#)
    - security impacts [6-1](#)
  - pushed archiving [1-35](#), [6-8](#)
- 
- ## R
- RAS
    - configuring
      - direct dial
        - engineering PC [4-28 to 4-31](#)
        - JACE-4/5 [4-14 to 4-16](#)
        - JACE-NP [4-20 to 4-25](#)

- ISP
    - JACE-NP [5-26](#)
    - installing, Windows NT 4.0 [4-27](#)
    - starting service
      - engineering PC [4-31](#)
      - JACE-NP [4-24](#)
  - RAS Server TCP/IP Configuration dialog box [4-23](#)
  - ras.properties
    - about [4-12](#)
    - configuring
      - captive ISP [5-10 to 5-15](#)
      - direct dial [4-14 to 4-16](#)
      - editing [5-13](#)
    - rasDebug parameter [4-14, 5-13](#)
    - rasEnable parameter [5-10](#)
    - rasMode parameter [5-10](#)
    - rate parameter [5-16](#)
  - RCMD
    - caution about station inoperability [2-6](#)
    - client component [2-5](#)
    - overview [2-5](#)
    - server component [2-5](#)
    - starting [2-6](#)
  - release directory, determining [6-12](#)
  - remote access server. See RAS
  - remote access services. See RAS
  - Remote Access Setup dialog box [4-20, 4-22](#)
  - remote command utility. See RCMD
  - Remote Desktop Sharing window [2-3](#)
  - remote printer notification [1-36, 6-8](#)
  - remoteAddr parameter [5-11](#)
  - repeaters [1-14](#)
  - required information, ISP [5-9](#)
  - RFC overview [1-37](#)
  - routers [1-15](#)
- 
- S**
- security
    - caution about enabling telnet [2-14](#)
    - firewall or proxy device [6-4 to 6-6](#)
    - guidelines
      - general [6-2](#)
      - JACE-4/5 [6-3](#)
      - Windows-based Niagara Hosts [6-3](#)
  - LAN/WAN [6-2](#)
  - Niagara considerations [6-1 to 6-4](#)
  - OS vulnerabilities [6-1](#)
  - packet sniffer [3-18](#)
  - public IP address [6-1](#)
  - using with Niagara hosts [6-1 to 6-26](#)
  - VPN [6-23 to 6-24](#)
  - Windows overview [3-5](#)
  - Security tab [4-38](#)
  - Select Distribution Directory dialog box [5-18](#)
  - selecting ISP [5-7](#)
  - serial and null modem cables and adapters, about [2-12](#)
  - serial connection, JACE-4/5 [2-7](#)
  - serial ports, configuring JACE-4 [4-10 to 4-11](#)
  - Server tab [4-36](#)
  - server-based networks, overview [1-3](#)
  - serverx parameter [5-23](#)
  - Services dialog box [4-24](#)
  - Services tab [4-20, 4-28](#)
  - servlets [6-5](#)
  - shell, about VxWorks target [2-8](#)
  - SNMP [3-5](#)
  - specialized servers, overview [1-3](#)
  - stacks, overview [1-12](#)
  - standard topologies, overview [1-3 to 1-6](#)
  - standards, IEEE 8.02 [1-10](#)
  - starting RAS service
    - engineering PC [4-31](#)
    - JACE-NP [4-24](#)
  - state [5-16](#)
  - static and dynamic IP addressing [1-25, 3-23, 5-2](#)
  - station monitor [1-36, 6-8](#)
  - station.properties file [6-11](#)
  - statusOutput parameter [5-16](#)
  - strong passwords, creating [6-3](#)
  - subnet masks
    - converting hexadecimal [3-20](#)
    - overview [1-20](#)
  - system architectures
    - direct dial [4-2 to 4-3](#)
    - ISP [5-2 to 5-5](#)
    - LAN [3-1 to 3-3](#)

system.properties file [2-14](#), [2-17](#)

## T

### tab

- Config [6-10](#)
- Details [4-42](#)
- General [3-8](#)
- Installation [5-18](#)
- IP Address [3-7](#), [6-22](#)
- Modems [4-26](#)
- Network [5-23](#)
- Network Settings [2-2](#), [3-13](#), [3-25](#), [4-10](#), [4-14](#), [5-9](#), [5-13](#)
- Protocols [3-7](#), [6-22](#)
- Security [4-38](#)
- Server [4-36](#)
- Services [4-20](#), [4-28](#)
- Users [3-6](#)

### target shell

- about [2-8](#)
- caution about station inoperability [2-8](#), [3-19](#), [3-21](#)
- commands [3-27](#) to [3-29](#)
- telnet connection [2-14](#)

### Target's Desktop

- menu [2-4](#)
- window [2-4](#)

### TCP/IP

- packet sniffer [3-18](#)
- utilities [2-20](#) to [2-26](#)

### TCP/IP and OSI

- application layer [1-17](#)
- data link layer [1-18](#)
- network layer [1-18](#)
- physical layer [1-18](#)
- presentation layer [1-18](#)
- session layer [1-18](#)
- transport layer [1-18](#)

### telnet [2-14](#)

- caution about enabling [2-14](#)
- enabling, JACE-4/5 [2-14](#)
- Hyperterminal [2-16](#)
- LAN connecting, JACE-4/5 [2-15](#)

### time synchronization

- changing default port [6-17](#) to [6-18](#)
- changing default port, impact [6-20](#)
- definition [6-17](#)

### token passing [1-13](#)

### tools [2-1](#) to [2-29](#)

- Admin Tool [2-1](#)
- configuration [2-1](#) to [2-19](#)
- connectivity troubleshooting [2-19](#) to [2-28](#)
- event log [5-19](#), [5-24](#)
- FTP [2-17](#)
- Hyperterminal [2-7](#)
- information resources [2-29](#)
- ipconfig [2-27](#) to [2-28](#), [3-31](#)
- JACE-NP remote control [2-2](#) to [2-7](#)
- NetMeeting [2-2](#)
- netstat [2-25](#) to [2-26](#)
- Notepad [6-14](#)
- nslookup [2-23](#) to [2-25](#)
- ping [2-20](#) to [2-22](#)
- RCMD [2-5](#)
- TCP/IP utilities [2-20](#) to [2-26](#)
- telnet [2-14](#), [2-15](#)
- tracert [2-22](#) to [2-23](#)
- Windows command-line utilities [2-20](#)
- Windows-specific [2-27](#)

### topologies, standard overview [1-3](#) to [1-6](#)

### tracert [2-22](#) to [2-23](#)

transmission control protocol. See TCP/IP

### transport layer [1-18](#)

### troubleshooting

- connectivity decision flowchart [3-15](#)
- connectivity tools
  - ipconfig [2-27](#) to [2-28](#)
  - netstat [2-25](#) to [2-26](#)
  - nslookup [2-23](#) to [2-24](#)
  - ping [2-20](#) to [2-22](#)
  - tracert [2-22](#) to [2-23](#)

### DDNS

- connections [5-24](#)
- update failures [5-25](#)
- determining lost IP address
  - general [3-16](#)
  - JACE-4/5 [3-19](#) to [3-21](#)
  - JACE-NP [3-17](#) to [3-19](#), [3-21](#)

DHCP

- lease renewal failure
  - JACE-4/5 [3-26](#)
  - JACE-NP [3-31](#)
- reservation not working
  - JACE-4/5 [3-26](#)
  - JACE-NP [3-31](#)

DNS tool [2-23 to 2-25](#)

ISP connection problems [5-19 to 5-21](#)

JACE connectivity [3-14 to 3-23](#)

network settings tool [2-27 to 2-28](#)

other access methods [3-21](#)

ports tool [2-25 to 2-26](#)

tunneling protocols [6-23](#)

twisted pair cables [1-7](#)

TZO

- about [5-22](#)
- registering [5-22](#)

---

## U

Unlock Workstation dialog box [2-4](#)

updateNvRamCmd parameter [4-14, 5-11](#)

updateNvRamFlag parameter [4-14, 5-11](#)

Users tab [3-6](#)

---

## V

Virtual Private Network dialog box [4-30](#)

VPN

- additional Niagara architectures [6-24](#)
- LAN [3-4](#)
- things to note [6-24](#)

- using with Niagara [6-23 to 6-24](#)

VxWorks target shell

- about [2-8](#)
- caution about station inoperability [2-8, 3-19, 3-21](#)
- telnet connection [2-14](#)

---

## W

WAN

- Niagara architectures [3-3](#)
- overview [1-2](#)
- things to note [3-4](#)

Web Supervisor

- configuring ISP [5-26](#)
- connecting multiple JACEs [4-6](#)
- specific security guidelines [6-3](#)

wide area network. See WAN

window

- Niagara Remote Installation [5-18](#)
- Remote Desktop Sharing [2-3](#)
- Target's Desktop [2-4](#)

Windows [4-29](#)

- domain [3-5, 3-6](#)
- Notepad [6-14](#)

Windows 2000 security overview [3-5](#)

Windows Internet naming service. See WINS

Windows NT 4.0

- installing RAS [4-27](#)
- security overview [3-5](#)

Windows NT 4.0 Workstation [1-32, 3-5](#)

Windows NT 4.0, Embedded [1-32, 3-5](#)

WINS [1-28, 3-5](#)

wireless networks [1-8](#)





