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

IT Manager's
FREQUENTLY ASKED QUESTIONS

This document addresses some of the common questions that IT managers have with using Tridium's Niagara Framework™ and products. It contains the following sections and questions:

Overview

Question 1 What is the Tridium product suite and the Niagara Framework?

Tridium offers a suite of Java-based products, powered by the revolutionary Niagara Framework, that are designed to integrate a variety of devices and protocols into a common distributed automation system. They incorporate the industry's first software technology to integrate diverse systems and protocols into a common object model, embedded at the controller level and supported by a standard web browser interface. The products enable monitoring and control systems to work together in a seamless web-enabled system. The monitoring and control systems can be based on LonWorks, BACnet, Modbus, and a wide range of legacy protocols. The suite also includes integrated network management tools to support the design, configuration, installation, and maintenance of interoperable control networks.

Question 2 What Niagara devices will be connected to or talking on my network?

Your Niagara installation may consist of one or more of the following devices (see Figure 1-1):

JACE Controllers—JACE (Java application control engine) controllers are hardware devices that provide integrated control, supervision, and network management services for networks of building monitoring and control devices. When connected over an Ethernet network using TCP/IP, JACEs can communicate with each other on a peer-to-peer basis as well as communicating with other Ethernet-based devices. With the optional Web User Interface (WebUI) service, a JACE can serve graphical views of the information contained in the connected devices to any standard web browser over the Internet or an intranet.

JACE controllers use one of two platforms:

- **JACE-NP**—compact PC with a conventional hard drive running an embedded version (or, optionally, a full version) of Microsoft Windows NT 4.0 Workstation and Microsoft Java Virtual Machine (JVM). The JACE-NP operates without a keyboard, monitor, or mouse.
- **JACE-4** and **JACE-5**—compact embedded processor platform with flash memory running Wind River VxWorks OS with either JWorks JVM or Jeode JVM.

Web Supervisor—The Web Supervisor is a network PC acting as a server for multiple connected JACE stations. The Web Supervisor provides efficient integration and aggregation of the information contained in multiple JACEs. In effect, the Web Supervisor creates a single view of these multiple devices, while providing database management, alarm management, and messaging services. The Web Supervisor software also contains the graphical user interface (WebUI service). The Web Supervisor can be connected to the Internet where the system's graphical views can be accessed using any standard web browser.

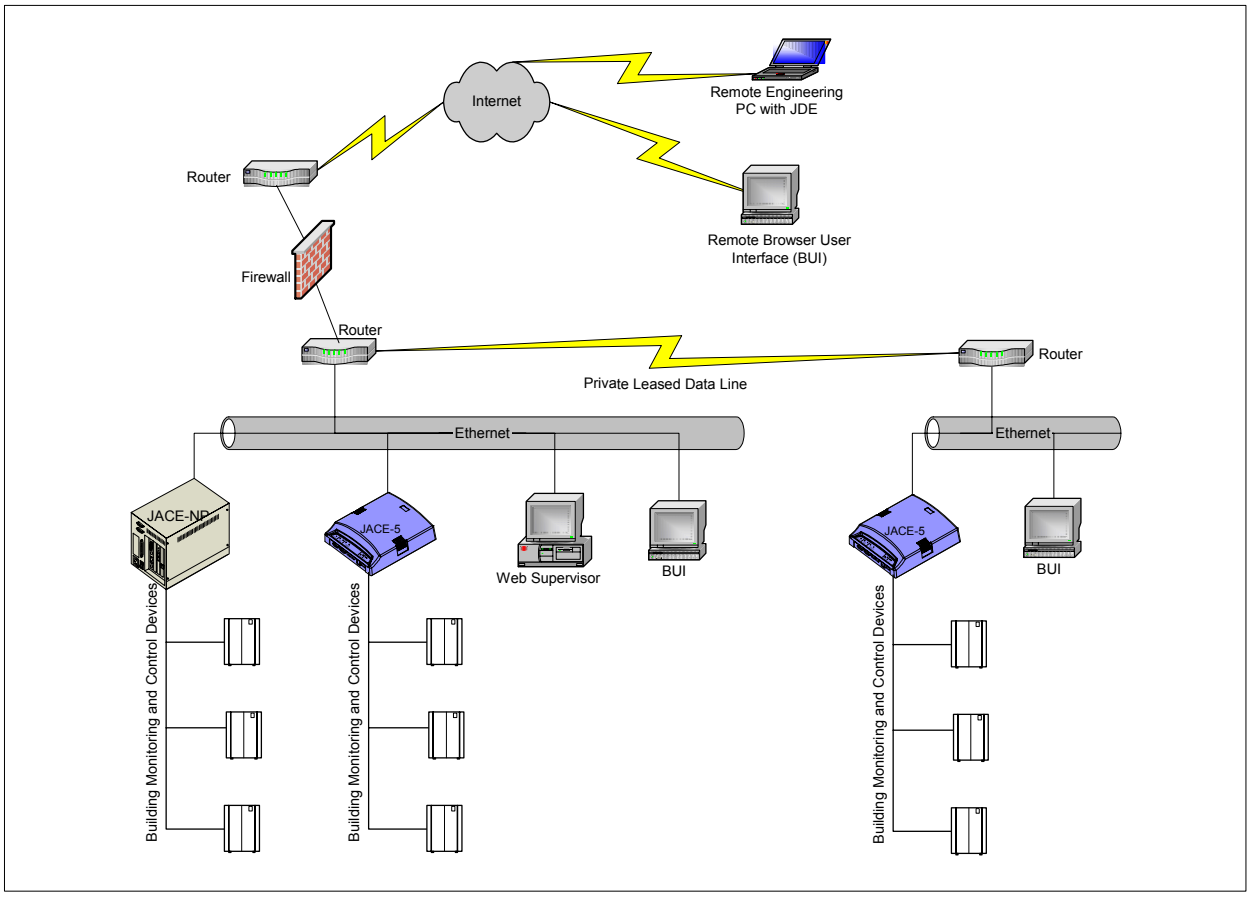
In addition, the Web Supervisor provides the engineering environment (the Java Desktop Environment, or JDE) used to create and maintain the station database. The Web Supervisor software and JDE are installed on a Windows NT 4.0 (Service Pack 4 or later) Windows XP Professional, or Windows 2000 PC.

Remote Engineering PC using the JDE (and Admin Tool)—The JDE is a comprehensive set of engineering tools combined into one common, easy-to-use graphical-based engineering environment. It simplifies the complexity of working with multiple protocols by consolidating them into one common object model. The JDE is the tool used to create and maintain the station database that runs on a Web Supervisor or JACE controller. The Admin Tool is used to set up and manage Niagara hosts. The JDE and Admin Tool are typically installed on a PC used by your systems integrator (SI) to maintain your on-site Niagara devices remotely across the Internet.

Browser User Interface (BUI)—The term BUI indicates user access of a Niagara station (JACE controller or Web Supervisor) using a web browser, such as Netscape Navigator or Internet Explorer. The BUI interface to Niagara provides remote administration and monitoring of building control systems on an intranet or over the Internet.

The following figure shows a typical Niagara architecture on a corporate WAN:

Figure 1-1 Typical Niagara architecture on a corporate WAN.



Integrating Niagara Devices into Your Environment

Question 3 How will the Niagara solution tie in with my current Windows NT Server/Windows 2000 infrastructure?

All of Tridium's Niagara products can co-exist on your Windows NT/Windows 2000 infrastructure. Since both the Web Supervisor computer and JACE-NP controller are built on the Windows platform, they will appear in your Network Neighborhood and can be browsed. At your discretion, the Web Supervisor computer can be a member of your Windows domain or Active Directory.

For more information, see the "Using Niagara in a Microsoft Windows Server Environment" section of the *Niagara Networking and Connectivity Guide*.

Question 4 Does Niagara support DHCP, DNS, and dynamic DNS?

DHCP is supported in all current versions of Niagara, though static IP addresses provide the most reliable connectivity. To reliably use DHCP we recommend that you reserve an IP address in the DHCP server for the MAC address of each Niagara device. This ensures that the Niagara device receives the same IP address whenever it requests one from the DHCP server.

DNS is supported in all current versions of Niagara, though the use of a HOSTS file on each Niagara station provides the most reliable connectivity to other Niagara hosts. With HOSTS files, there is no dependency on a remote DNS server for name resolution.

DDNS *directly* to a network server is available for Web Supervisors running Windows 2000, but is not supported on our other devices. The JACE-4/5 series controllers support DDNS through an Internet provider when connecting to your site through an ISP.

For more information, see the "Available Networking Technologies" topic of the *Niagara Networking and Connectivity Guide*.

Question 5 Which software protocols and RFCs (Request for Comments) does Niagara support?

Niagara primarily uses the HTTP protocol to communicate between Niagara hosts. We support version 1.1 (RFC 2616).

We support the following optional software protocols:

- SMTP (as a client for e-mail alarm notifications)—RFC 821
- Time protocol (as a client or server for time synchronization)—RFC 868
- SNMP version 1 and 2—RFCs 1155, 1157, 1902, 1905, and 1906 (not all functions of these RFCs supported)

For information about the protocols supported in our OS platforms (Microsoft Windows NT 4.0, Windows 2000, Wind River VxWorks 5.4) contact the respective OS vendors.

Question 6 I use Netscape Navigator as a browser, are there any ActiveX compatibility issues that I need to be concerned with?

We do not use any ActiveX in our software. However, Systems Integrators (SIs) can implement this technology when they develop the browser GUI. To prevent this you can either:

- specify that the browser GUI must not include the use of any ActiveX components.
- specify that the SI make the GUI compatible to Netscape Navigator (which does not support ActiveX).

Managing Niagara Hosts

Question 7 How do I back up this device?

Our application includes a backup service that can be used to back up any Niagara system that archives data. Typically these are Web Supervisors and JACE-NPs with the database service (for more information on this function, see "Archiving," page 6).

The backup service copies the station directory (including the archive database) into a WinZip-compatible file on a daily basis. The zip file is placed in the ***<niagaraRelease>*\backups*<stationName>*** directory. Two backups are stored: the most recent (backup.zip) and the one prior (backupOld.zip). We recommend that you use your standard host backup method to back up these files to removable storage on a daily basis.

Question 8 What LAN network management tools do I use to manage these devices?

The Niagara application provides all the tools required to manage our devices (typically the JDE and Admin Tool).

The optional SNMP module allows limited monitoring and management of Niagara devices. The SNMP modules provides more robust monitoring and management of building monitoring and control devices.

Impacts on Network Traffic

Question 9 When does a JACE controller communicate with the Web Supervisor and vice versa?

Table 1-1 provides a summary of the most common types of communication between hosts in a Niagara installation. Included is the host that initiates each type of communication, the host that receives it, and a description of the function.

Table 1-1 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: • for viewing real-time control information • for maintaining a station (through the use of servlets) • viewing station data (logs, alarms, schedules, etc.)
Station and Host Administration	Java Desktop Environment (JDE)	Web Supervisor or remote PC of System Integrator (SI)	Any Niagara host	Connection for the purpose of creating and maintaining a live station. Typically performed by your SI.
	Admin Tool	Web Supervisor or remote PC of System Integrator	Any Niagara host	Connection for the purpose of changing host configuration, adding users to the host, installation of a station, software or licenses, or database administration. Typically performed by your SI.
Archiving	Pushed archiving	Any Niagara host set to remotely archive logs	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.
Alarming	Alarm archiving	Any Niagara host set to remotely archive alarms	JACE-NPs and Web Supervisors running the Database service	Communication from the initiating host to send alarms to a host set up to archive the alarms (and typically, which runs the Alarm Console for acknowledgement).
	Alarm Console acknowledgement	Web Supervisor	A Niagara host with alarming set up to archive local	Connection from the Web Supervisor to acknowledge an alarm on the host archiving the alarm.
Global data passing		Any Niagara host	Any Niagara host	Connection from one host to another to exchange real-time data via interstation (external) 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 verifying network connectivity. If the ping fails over time, produces a station alarm.

For more information on some of the less common Niagara functions, see Table 1-13 in the *Niagara Networking and Connectivity Guide.*

Question 10 What does a system of JACEs and a Web Supervisor do to my network traffic and bandwidth?

Table 1-2 lists each typical communication function, with its associated bandwidth impacts.

Table 1-2 Bandwidth impacts of communication between Niagara hosts.

Communication	Typical Initiating Host (Client)	Receiving Host (Server)	Bandwidth Impacts
Browser User Interface (BUI)	Any host	Any Niagara host	**GxPages** • **Downloading of applet to BUI client**—8403 bytes plus 30% for HTTP overhead. Also add size of graphics, which download on page change, and are cached in the browser for reuse (cache time is based on browser settings). A typical VAV graphic is 90 kilobytes to download. • **Browser updates**—the server sends updates when a value changes. Each update packet is 62 bytes plus 26 bytes per value. A typical value update sends about 400 bytes every 3 to 5 seconds. **Note:** These figures are estimates of the volume of traffic when using Internet Explorer. **Text-based Pages** • **Page size**—500 bytes plus size of page. Size of page varies greatly by type of page and amount of data on each page (such as for an alarm page), which can vary. • **Updates**—Pages do not automatically refresh. A manual refresh sends the entire page. **Considerations for both** • **Keep alive messages**—When a BUI connection is idle, a message is sent from client to the server every 250 milliseconds. The message is 60 bytes with a 62-byte response.
Java Desktop Environment (JDE)	Engineering PC	Any Niagara host	• **Actively engineering a station**—the traffic on average is 1600 bytes per second (bps), however it can spike at much higher levels. • **Keep alive messages—**When the JDE is idle, a message is sent from client to server every 5 seconds. The message is 60 bytes with a 62-byte response.
Admin Tool	Engineering PC	Any Niagara host	

Table 1-2 Bandwidth impacts of communication between Niagara hosts. (continued)

Communication	Typical Initiating Host (Client)	Receiving Host (Server)	Bandwidth Impacts
Pushed archiving[1]	Any Niagara host	JACE-NPs and Web Supervisors running the Database service	Logs set up to push archive can be set to archive daily (sending all records for the last 24 hours) or "near full" (when the size of the log buffer is almost exhausted). A smaller log buffer set to archive "near full" sends a smaller amount of data more frequently. A larger log buffer set to archive daily sends a larger amount of data, at a configurable time (typically off-hours). The data rates for each type of log are as follows: • **Analog logs**—217 bytes plus 16 bytes per record in buffer • **Binary logs**—243 bytes plus 13 bytes per record in buffer • **String logs**—243 bytes plus 13 bytes per record in buffer • **Integer logs**—250 bytes (average) plus 16 bytes per record in buffer • **Multi-state logs**—250 bytes (average) plus 16 bytes per record in buffer **Note:** Multi-state data size varies based on the amount of text in the *stateText* field.
Alarm archiving[1]	Any Niagara host with notification set to archive_remote	JACE-NPs and Web Supervisors running the Database service	The size of the alarm archive varies depending on the amount of alarm text and the options enabled on the object. The average data transfer is 1000 bytes per alarm.
Alarm Console acknowledgement	Web Supervisor (typically)	A Niagara host set up to archive alarms at the Web Supervisor	The size of the acknowledgement is approximately 1000 bytes.
Global data passing (interstation links)	Any Niagara host	Any Niagara host	• **Start up of station**—When the receiving host starts up, it sets up the connection to the initiating host. This set up sends 700–1000 bytes per link. • **Data updates**—The station property *interstationSendTime* controls how often data is pushed to the receiving host. By default, a data set with all updated values is sent every 5000 milliseconds. The size of the data set is 112 bytes + 14 bytes per analog value + 11 bytes per binary value. • **Keep alive messages**—A message is sent from client to server every 5 seconds, if data is not sent on a more frequent interval. The message is 60 bytes with a 62-byte response.
Station monitor	Any Niagara host	Any Niagara host	A UDP message of 60 bytes is sent at 10-second intervals. The responding station returns a response that is 42 bytes + 1 byte per character in the station name (for a maximum of 62 bytes/message).

1. This communication stream uses a special connection from client to server. If a connection is active at the time the data is passed, the stream will use the existing connection. Otherwise, a new connection consumes 1200 bytes in a total of 15 packets.

Your Niagara Systems Integrator and Tridium will work with you to properly configure your system to ensure minimal impact to your networking environment.

Connecting Niagara Hosts on the Internet

Question 11 How do I access a JACE or Web Supervisor over the Internet?

If Internet access is a requirement, the JACE or Web Supervisor must have a public (routable) IP address. You can assign one from your pool of public addresses, or use name/address translation (NAT) through a firewall or router to assign an address. See also the "Impacts on Security" section.

Question 12 Can I access the entire Niagara network if only the Web Supervisor is exposed to the Internet?

Your SI can design your Niagara system to allow you to manage your facility's control equipment through one Web Supervisor with a public IP address. Interstation links from any JACEs with private IP addresses to the exposed Web Supervisor can provide integration and aggregation of the information contained in the JACEs.

However, if your SI needs to maintain individual JACEs that are using private IP addresses on your network, you would need to implement at least one of the following:

- provide on-site network connectivity to the SI.
- provide a telephone line for direct dial into Windows RAS on a Web Supervisor or JACE-NP. Once dialed into the Niagara device the SI can reach the additional Niagara devices.
- provide another (non-Niagara) dial-up solution into your network.
- provide access to the Web Supervisor via remote control software. The SI can use the JDE on the Web Supervisor to manage the other hosts.
- provide VPN connectivity to the SI (see Question 15.)

Impacts on Security

Question 13 How will Niagara tie in to my security policy?

There are three aspects of security for any Niagara device:

- **Licensing security—**Each Niagara device (JACE, Web Supervisor, remote engineering PC) has a license file that is specific to the machine that it resides on. The file is digitally signed so that it cannot be changed or used on another Niagara device.

  Within the license file:

  – The **orgId** field identifies and controls which company is licensed to use the JDE software. This is typically assigned to the SI that installs your Niagara system. The orgId on a PC using the JDE must match the orgId of any Niagara device (JACE or Web Supervisor) that it is engineering.

  - The **projectId** identifies the project. This is typically assigned to your company. The projectId of two or more stations much match for those stations to share data.

  You can request that the orgId be specific to your company and not the orgId of the installing SI. By doing this, you control which SI (if any) can have an engineering PC licensed with your orgId.

- **Host authentication**—The device is accessed at the host level for maintenance functions such as installing and upgrading the stations and the OS, changing of network settings, and setting system time.

  Host access to the Niagara system is provided by local authentication on the Web Supervisor or JACE (both platforms). The Niagara device uses a local workstation account that does not participate in domain or Active Directory authentication, so there is no additional security burden on your existing domain or Active Directory infrastructure. NT-based Niagara devices can support your current policies for host-level access.

- **Station authentication**—The station database has separate layer of security for user-to-station and station-to-station access.

  Niagara uses a proprietary authentication scheme that uses local user names and passwords defined on each station. Optionally, Niagara station user names can be configured with strong passwords. With strong passwords, a station user password must meet the following minimum requirements:

  - Eight (8) characters in length
  - one (1) alphabetic character upper case
  - one (1) alphabetic character lower case
  - one (1) special character (!@#$%_0123456789)

Question 14 How is the JACE protected from viruses?

The Niagara devices function as proprietary web servers, not typical client machines. As part of normal station operations, they do not download any files. However, you may want to install virus protection for a Web Supervisor PC if it is used for other (non-Niagara) functions.

Question 15 How do I protect someone from hacking into my Niagara system?

Concerns about hacking typically fall into three categories:

- **Viruses**—See Question 14.
- **Web Servers**—The Niagara Framework does not use the Microsoft IIS server, instead it is a pure Java web server developed by Tridium. This eliminates many security holes associated with the Microsoft IIS server. Our software uses a proprietary protocol running on top of HTTP. Without our software it is highly unlikely that someone could hack our system without reverse engineering our product.

- **Host Access**—Any host connected to the Internet is vulnerable to attacks. If your Niagara host has a public IP address and is reachable from the Internet, there are two suggested routes for additional security:
  - **Using a Virtual Private Network (VPN).** Using a VPN allows for tunneling traffic from both the BUI user and off-site SI into your organization. All messages are encrypted, including the user names and passwords used to access the system either as a browser user, or for JDE/Admin Tool maintenance use. See Question 16.
  - **Using a Firewall.** A firewall can be used to limit access to specific ports on our equipment. See Question 17.

For more information on securely using our equipment, see the "Security Considerations" topic of the *Niagara Networking and Connectivity Guide*.

Question 16 How do I set up/use a VPN?

Tridium offers professional services to help end users and system integrators configure VPNs for their Niagara environments.

Question 17 How does your system work with firewalls and proxy servers?

Both the JACE and the Web Supervisor can use NAT (name/address translation) through a firewall to expose them to the Internet. The firewall should be used to filter traffic at the port level to any exposed Niagara device. Our application primarily uses the following ports for communication with devices typically located outside the firewall:

- **80**—for BUI, JDE, and Admin Tool traffic, and many station-to-station functions.
- **3011**—for the Admin Tool (and some browser-based maintenance) traffic.

These are the standard port numbers used for most functions; they can be changed to fit your individual security requirements.

In addition, the following optional ports are also used by our equipment. Typically these ports are in use between stations located behind the firewall:

- **37**—when a Niagara host is acting as an Internet Time Protocol server or client.
- **21**—for alternate maintenance access (FTP) to JACE-4s and JACE-5s.
- **23**—for alternate maintenance access (telnet) to JACE-4s and JACE-5s.
- **25**—used for client connections to a mail server for e-mail notifications.
- **522, 1503, 1731**—for desktop (NetMeeting) access to JACE-NPs using the embedded OS.
- **139**—for command-line (RCMD) access to JACE-NPs using the full OS.

Your SI can advise you if they want you to open any of these additional ports.

Lastly, the following two things also impact our use with a firewall:

- In order for a BUI user to use our application, the firewall must allow downloading of Java applets to the BUI client.

- In certain instances, the JDE may have trouble working through some firewalls or proxy servers. To avoid this you can either:
  - configure the firewall to filter only at the port level to the Niagara device.
  - secure the MAC or IP address of the SI machine using the JDE and allow all traffic between that host and the Niagara device.

For more information on securely using firewalls with our equipment, see the "Using a Firewall or Proxy Device" section in the *Niagara Networking and Connectivity Guide*.

Question 18 What firewalls does your system work with?

Any firewall that performs NAT and filters at the port level works with our products. We use Cisco PIX firewalls at all of our Tridium facilities and are working behind various firewalls at our client locations.

More Information

The "Niagara Networking and Connectivity Guide," referenced throughout this document, is available from your System Integrator.