

Information and/or specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein are covered by one or more U.S. or foreign patents. This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, 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. Complete Confidentiality, Trademark, Copyright and Patent notifications can be found at: <http://www.tridium.com/galleries/SignUp/Confidentiality.pdf>.

JACE, Niagara Framework, Niagara AX Framework and the Sedona Framework are trademarks of Tridium, Inc.

GPRS modem option

During the AX-3.4 development cycle, a GPRS (General Packet Radio Service) cellular modem option card became available for newer JACE controllers. For the recent “M2M JACE” platform, an *onboard* GPRS cellular modem option is also available. This document provides software configuration details related to the use of this JACE option. Included is the necessary JACE platform configuration, as well as SMS (Short Message Service) application and details about the GprsPlatformService. A reference section on the platform [GPRS Modem Configuration view](#) is also included.

- For details about *other* platform views of a JACE, see the *NiagaraAX Platform Guide*.
- For GPRS modem option card and antenna mounting instructions, see the *GPRS Modem Option Installation Sheets* document, which ships with the option card. For details about the operation of the two LEDs on the GPRS modem option card, see “[GPRS modem LEDs](#)” on page 10.
- For details on M2M JACE mounting and wiring, including its GPRS modem option and antenna, refer to the *Mounting and Wiring* document that ships with that JACE. For operation details on its single “GPRS” Status LED, see “[GPRS modem LEDs](#)” on page 10.

An appendix provides details specific to using the GPRS modem option with the Wyless Group (Wyless) as the wireless [service provider](#). Topics include connectivity options, connecting as a VPN client, and an example IPsec VPN gateway configuration.

Note: *Once the GPRS modem option is installed and connects to the service provider, in some scenarios you may no longer be able to communicate to the JACE via the hardwired Ethernet LAN connection, unless your PC is on the same logical subnet as the JACE. This is a “dual NIC consequence” that may occur when the “always on PPP” mode of the GPRS modem is enabled. The actual outcome is dependent on a combination of several factors, and include both the IP configuration of the local network as well as the IP configuration of the connected service provider’s mobile network (in the case of Wyless, a VPN network). In general, avoid any “IP address range overlap” between the JACE’s local network and the service provider’s network.*

The following main sections are in this document:

- “[Service Provider](#)” on page 2
- “[Use cases for GPRS equipped JACEs](#)” on page 2
- “[Required platform GPRS setup](#)” on page 5
- “[About the GprsPlatformService](#)” on page 8
- “[SMS application for GPRS](#)” on page 8
- “[GPRS modem LEDs](#)” on page 10
- Reference section about “[GPRS Modem Configuration view](#)” on page 11
- “[Document change log](#)” on page 17
- Appendix: “[Wyless as service provider](#)” on page 18
 - “[GPRS connectivity overview](#)” on page 18
 - “[Connecting as a VPN client to a JACE with GPRS modem option](#)” on page 19
 - “[Configuring an IPsec VPN gateway to access a VPN network](#)” on page 21

Service Provider

Any GPRS modem option for a JACE controller requires a SIM (Subscriber Identity Module) card that has been provisioned by a wireless *service provider*. Typically, the customer (i.e. Niagara system owner) contracts with this provider for a defined amount of data transfer (in MB), at some monthly cost.

- Currently, the Wyless Group is the only Tridium-approved service provider in the continental U.S., and thus the only supported SIM card source. In addition, development and testing of the GPRS modem option used Wyless provisioned SIMs. However, it is possible that other wireless service providers may be approved in the future. Note that an appendix in this document provides details specific to Wyless—see “[Wyless as service provider](#)” on page 18.
The GPRS modem option is available bundled with a Wyless SIM (NPB-GPRS-W). Also available separately are the GPRS modem option without a SIM (NPB-GPRS), or a Wyless SIM card alone (GPRS-SIM-W).
- Service provider connection costs and plan differences are currently outside the scope of this document. Consult your Tridium sales representative for more information on these items.
- In turn, the service provider typically subcontracts with a cellular operator to provide network coverage. In the case of Wyless in the U.S., this operator may be T-Mobile USA. The name of the cellular operator may appear on the SIM card, however, the system (JACE) owner deals only with the service provider for all billing, as well as all required support.

As the name implies, each SIM card contains a number of unique IDs and associations. See the next section “[SIM](#)” for more details.

SIM

The [Service Provider](#)-provisioned SIM card installs in a connector on the GPRS modem option board.

Along with each SIM card, the service provider supplies its provisioned:

- SIM ID — a 19-digit number unique to this one card.
- Provider APN — Access Point Name for the cellular provider network. The APN specifies the gateway between the provider’s mobile network and the Internet.
- APN credentials - Username and password for authentication to the APN.
Note: Be sure to get the username and password from the service provider (Wyless, for example). This is required for the GPRS modem to make the PPP connection.
- Phone number - Associated phone number (seen in any SMS messages sent by a hosted station).
- Private IP address — Static IPv4 address within a private address space of the VPN wireless network.
Note: True if a Wyless SIM, other service providers may or may not supply a fixed IP address.
- IMSI — (International Mobile Subscriber Identity) a unique 15-digit GSM mobile device identity. You use the supplied APN name and credentials in the platform configuration of the GPRS modem option (its SIM ID is automatically recognized). See “[Required platform GPRS setup](#)” on page 5.

In the case of Wyless as service provider, its associated private IP address is how you can connect to the JACE over the Internet using the service provider’s VPN (Virtual Private Network). See the first appendix section “[GPRS connectivity overview](#)”.

Use cases for GPRS equipped JACEs

The following sections illustrate possible “use case” scenarios for GPRS modem-equipped JACEs.

Note: For all use cases, GPRS connection speeds are similar to dialup modems—typically 30 - 60Kbps download, and 10 - 15Kbps upload. Therefore, JACE operations such as software upgrades are not recommended. Instead, a direct connection (to LAN1 or LAN2 port of the JACE) should be used when a large transfer of data is needed.

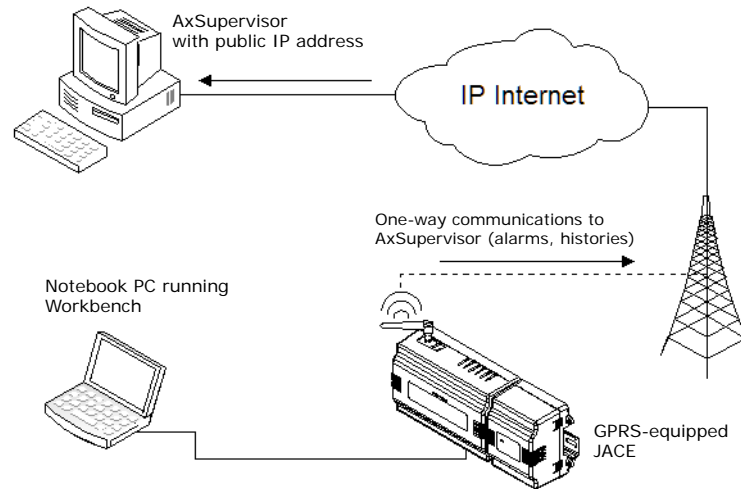
1. [One-way JACE communications to AxSupervisor](#)
2. [One-way JACE communications with alarm “hopping”](#)
3. [Temporary two-way connection using VPN client software](#)
4. [Permanent two-way connection using IPSec VPN gateway](#)
5. [Supervisory GPRS JACE to subordinate GPRS JACE](#)

Note: These use cases reflect Tridium test scenarios, using Wyless as the [Service Provider](#). A future revision of this document may provide more specific details/notes about system operation in these different examples.

One-way JACE communications to AxSupervisor

In this use case, the AxSupervisor must have a public IP address. The GPRS-equipped JACE can initiate communications to the AxSupervisor for alarms and exporting histories.

Figure 1 One way communications from JACE to AxSupervisor

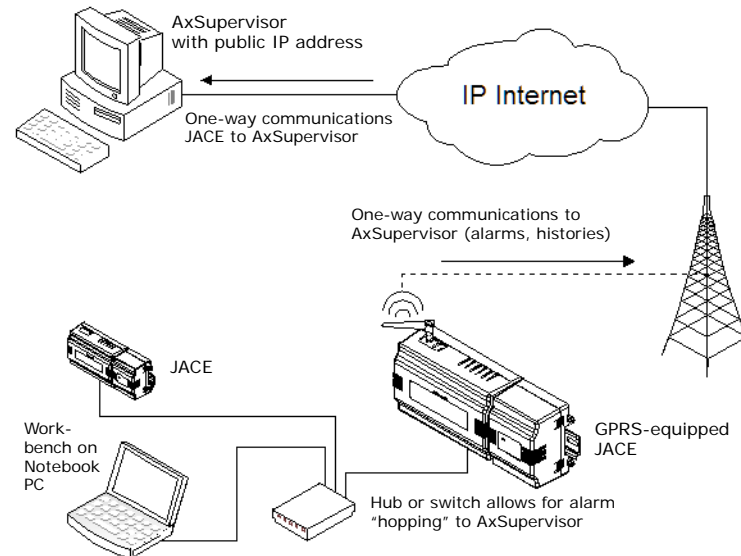


As shown in Figure 1, a notebook PC running Workbench can attach directly to the Ethernet port on the JACE. This type of connection is needed to perform JACE platform maintenance (upgrades, etc.).

One-way JACE communications with alarm “hopping”

In this use case, the AxSupervisor must have a public IP address. The GPRS-equipped JACE can initiate communications to the AxSupervisor for alarms and exporting histories. Note that the addition of the hub or switch connecting the remote JACEs also allows for alarm “hopping” to the AxSupervisor.

Figure 2 One way communications from JACE to AxSupervisor with remote alarm “hopping”

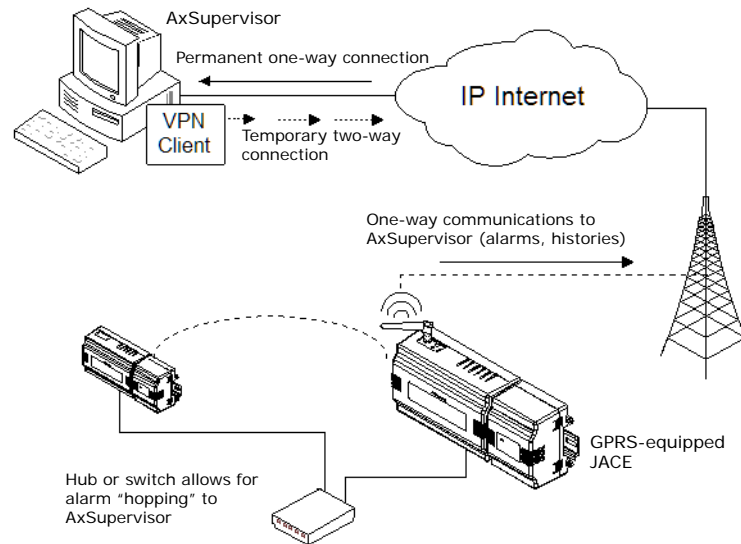


As shown in Figure 2, a notebook PC running Workbench can attach directly to the hub of the remote JACEs. This type of connection is needed to perform JACE platform maintenance (upgrades, etc.).

Temporary two-way connection using VPN client software

In this use case, the Workbench PC can use VPN client software to make a temporary PPTP connection to the GPRS-equipped JACE (either for a platform connection, or to open its station). As in the previous use cases, the GPRS-equipped JACE can also initiate communications to the AxSupervisor for alarms and exporting histories (again, the AxSupervisor must have a public IP address).

Figure 3 Temporary platform/station connection using VPN client software



As shown in [Figure 3](#), the addition of the hub connecting the remote JACEs also allows for alarm “hopping” to the AxSupervisor.

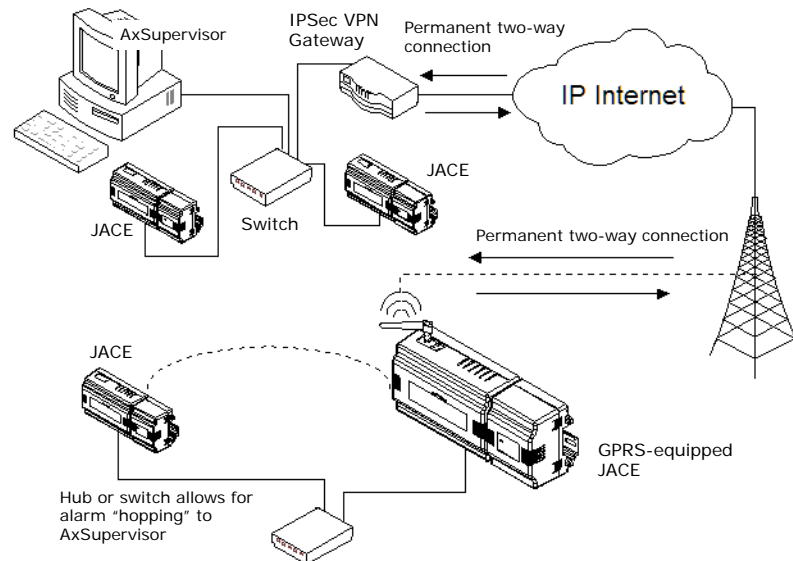
For related details, see [“Connecting as a VPN client to a JACE with GPRS modem option”](#) in the [“Wyless as service provider”](#) appendix.

Permanent two-way connection using IPSec VPN gateway

In this use case, a permanent connection to the GPRS-equipped JACE is provided via an IPSec VPN gateway, configured in cooperation with the Service Provider. This allows a *remote* JACE (or JACEs) to be included in the NiagaraNetwork on the AxSupervisor’s station, along with local JACEs.

Note: A local GPRS-equipped JACE is not supported.

Figure 4 Permanent two-way connection using configured IPSec VPN gateway



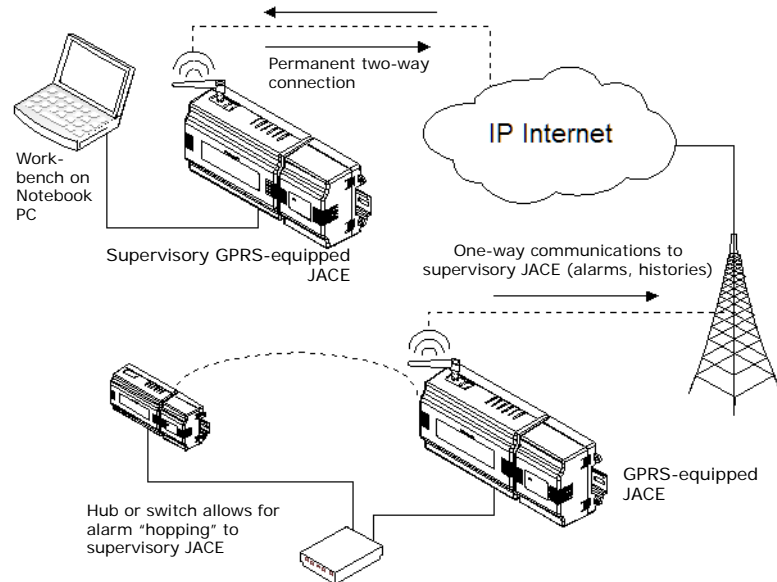
As shown in [Figure 4](#), the addition of the hub connecting the remote JACEs also allows for alarm “hopping” to the AxSupervisor.

For related details, see [“Configuring an IPSec VPN gateway to access a VPN network”](#) in the [“Wyless as service provider”](#) appendix.

Supervisory GPRS JACE to subordinate GPRS JACE

In this “mobile-to-mobile” use case, a permanent connection between a GPRS-equipped *supervisory* JACE is maintained to a subordinate GPRS-equipped JACE.

Figure 5 Mobile-to-mobile connection between GPRS-equipped JACEs



As shown in Figure 5, the addition of the hub connecting the remote subordinate JACEs also allows for alarm “hopping” to the supervisory JACE.

Required platform GPRS setup

As the first stage of configuration for any GPRS modem option application, each JACE equipped with a GPRS modem option requires the following key configuration properties defined in the [Provider](#), [Modem](#), and [SMS](#) Configuration sections of its **GPRS Modem Configuration** platform view.

- Also see “[TCP/IP configuration with GPRS modem](#)” on page 7 about *not specifying* DNS servers.
- Refer to the NiagaraAX Platform Guide for more information about a platform connection, as well as all other platform views. Additional reference information about the **GPRS Modem Configuration** view can be found in this document, see “[GPRS Modem Configuration view](#)” on page 11.

Note that in the station running on the JACE, there is also a “GprsPlatformService” dynamically created under its PlatformServices container. This platform service provides a number of read-only (status) properties, but is not used in configuration. For details, see “[About the GprsPlatformService](#)” on page 8.

Key Properties: Provider Configuration

Along with a SIM card, the [Service Provider](#) should furnish three pieces of data you need to enter in the “Provider” section of the JACE platform’s GPRS Modem Configuration view (Figure 6).

Figure 6 Provider Configuration section of GPRS Modem Configuration platform view

The screenshot shows the 'Provider Configuration' section of a software interface. It contains several configuration options with checkboxes and input fields. The 'Provider APN' field is set to 'telargo.t-mobile.com'. The 'APN User Name' field is set to 'Trib015'. The 'APN Password' field is masked with dots. The 'Type of authentication for ppp' is set to 'PAP'. The 'Min time before reconnecting ppp' is set to '00000h 03m 00s'. The 'Max ppp Idle Time before disconnecting ppp' is set to '00000h 30m 00s'. The 'Max Number of times LCP can fail before modem reset' is set to '10'. Green arrows point to the 'Provider APN', 'APN User Name', and 'APN Password' fields.

Note: Be sure to get the APN User Name and Password from the service provider (Wyless, for example). This is required for the GPRS modem to make the PPP connection.

- Provider APN — The APN (Access Point Name) for the cellular provider network. This specifies the gateway between the mobile network and the Internet.
- APN User Name — User name to authenticate to the provider's network.
- APN Password — Password for the above user, to authenticate to the provider's network.

Above these APN-related properties are three checkboxes that apply to the PPP (Point-to-Point Protocol) stack used by the GPRS modem, described as follows:

- Enable On-Demand PPP — Typically, you leave this cleared (disabled) for “always connected” PPP. Generally, this is enabled only if you are “pushing” *all* data from the JACE, such as when you care *only* about sending alarms/alerts. This results in less bytes sent (and billed), rather than maintaining a constant PPP connection. However, if data must be available for subscriptions—say, browser access to Px views, or there is proxied data in other stations, this checkbox must be cleared (disabled). **Note:** *If only occasional access to data/Px views is needed, you could configure for on-demand PPP. In this case, when needed you could send the JACE's GPRS modem explicit SMS messages to start up PPP and send back its IP address. This data could then be used to connect to it via the VPN network. For related details, see “Remote SMS commands” on page 9.*
- Enable PPP Debug — Typically, you clear (disable) unless you are diagnosing PPP authentication or parameter issues.
- Switch gateway on ppp connection — Typically, you leave this enabled (checked), unless the AxSupervisor is on the same local LAN as the JACE.

Finally, review settings of the following four properties:

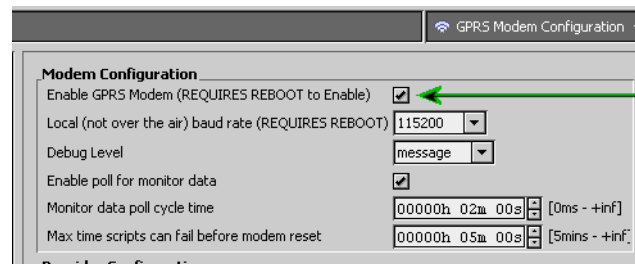
- Type of authentication for ppp — Either CHAP or PAP for Wyless (Service Provider dependent).
- Min time before reconnecting — This value guarantees that the pppd (PPP daemon) cannot respawn for this amount of time, providing a minimum down time, with a default value of 3 minutes. Typically left at default. Recommended not to be set under a minute, to allow for GPRS de-registrations, etc. to take effect. Typically of interest only when transmitted byte counts are of primary importance.
- Max ppp idle time before disconnecting — A value passed to the pppd when spawned, with a default value of 30 minutes. Typically left at default, after this amount of time with no data in the “PPP pipe,” the PPP connection is broken down, so it does not have to be maintained. This counter resets whenever PPP traffic occurs.
- Max Number of times LCP can fail before modem reset — Default value is 10, range is from 2 to 100. Typically left at default, unless otherwise directed by Systems Engineering.

Note: For additional details on these platform Provider Configuration properties, see the section “Provider Configuration” on page 12.

Key Properties: Modem Configuration

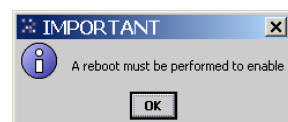
In the Modem Configuration section of the JACE's platform **GPRS Modem Configuration** view (Figure 7), you must enable the modem. Often, you can leave other properties at default values.


Figure 7 Modem Configuration section of GPRS Modem Configuration platform view



When you check the Enable box, a popup dialog informs you that a JACE reboot is necessary for the enable to become effective, as shown in Figure 8.

Figure 8 Popup dialog when enabling modem



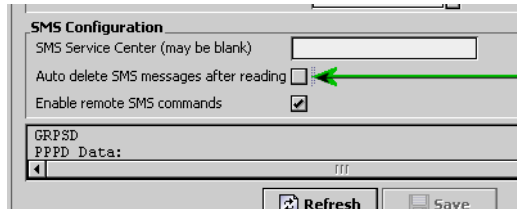
Clicking **OK** closes this dialog, and you can continue editing. After you Save  any configuration changes, you will need to expressly reboot the JACE for the GPRS modem to become enabled. Likewise, if you later disable the GPRS modem, a corresponding popup dialog informs you a reboot is necessary.

Note: For additional details on other platform Modem Configuration properties, see the section “[Modem Configuration](#)” on page 12.

Key Properties: SMS Configuration

Depending if the JACE is running a station using the SmsService, the “Auto delete SMS messages after reading” property in the SMS Configuration section ([Figure 9](#)) should be set differently. By default, auto delete is disabled (checkbox cleared).

Figure 9 SMS Configuration section of GPRS Modem Configuration platform view



- If *not* using the SmsService, then make sure to select (check) “Auto delete SMS messages after reading.” This keeps any possible “SMS spam” from filling the buffer on the GPRS modem, which could prevent receiving additional SMS messages—including possibly-needed remote SMS commands.
- If using the SmsService, disable (clear) this platform configuration to auto delete SMS messages. Instead, in the station’s SmsService (in Transport), configure “Delete Read Messages” to be true. This lets the SmsService read/process messages *before* they are deleted in the GPRS modem’s buffer.

Other SMS related configuration properties include the following:

- SMS Service Center — Leave blank for Wyless (note this is [Service Provider](#) dependent).
- Enable remote SMS commands— Enable (check) if you require the ability to send SMS commands to the GPRS modem from a cell phone. See “[Remote SMS commands](#)” on page 9 for related details.

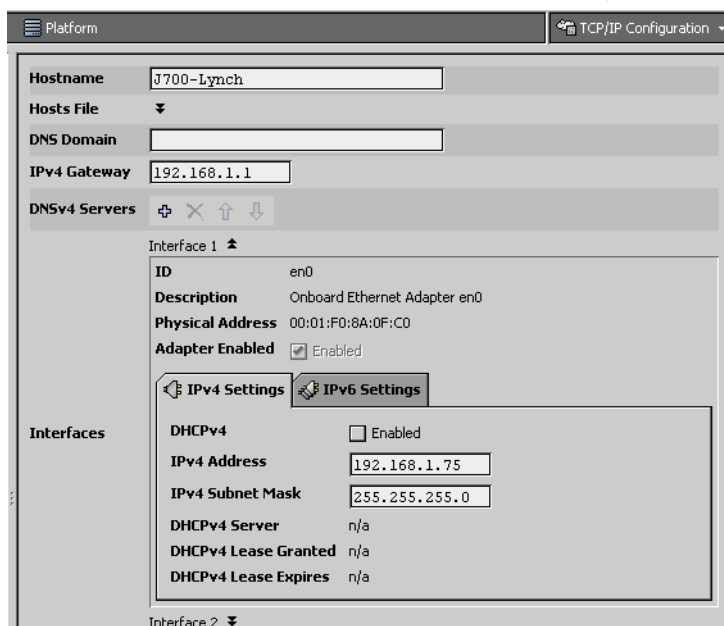
Note: For additional details on platform SMS Configuration properties, see the section “[SMS Configuration](#)” on page 13.

TCP/IP configuration with GPRS modem

Note that in the JACE’s platform TCP/IP configuration, *no DNS servers should be defined*—otherwise, the GPRS modem will not function. The intended application for a GPRS modem is on a site where no DNS servers can be reached on the local Ethernet network, or where no local Ethernet network exists.

Note: Also, it is recommended to not use DHCP on any Ethernet adapter when the GPRS modem option is used. [Figure 10](#) shows an example JACE’s platform TCP/IP configuration view, where *no* DNSv4 servers are defined, and DHCPv4 is *not* enabled.

Figure 10 Do not define DNS servers nor enable DHCP (on any Ethernet adapter)

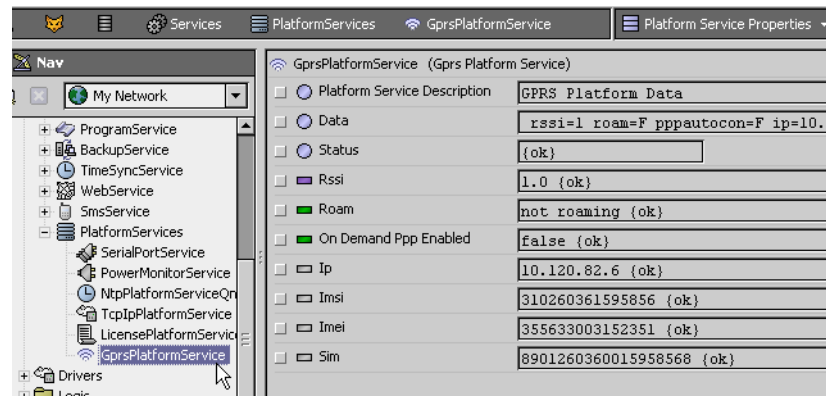


About the GprsPlatformService

Provided that the JACE has the GPRS modem option installed, along with the platGprs module, and the GPRS modem is platform-enabled in the JACE, any station running on it includes a “GprsPlatformService” under its PlatformServices container (Figure 11).

Note: For general information about a station's PlatformServices, refer to the section “About Platform Services” in the NiagaraAX Platform Guide.

Figure 11 GprsPlatformService appears under PlatformServices in station running on JACE



All properties in the Gprs Platform Service are read-only status types, and include the following:

- **Platform Service Description**
Text string from lexicon key “GprsPlatformService.description”.
- **Data**
Results returned from reading “/dev/gprs/data”, concatenated into a single text string. Includes properties and values below starting with Rssi through Imei. If a read error occurs with this file, it will indicate a message similar to “resource manager UnresolvedException”.
- **Status**
Either {ok} or {fault}. If “/dev/gprs/data” is available and readable, then {ok}. If gprsd is not running (or it has shut down/not started for some reason), then {fault}.
- **Rssi**
Received signal strength indicator (i.e. number of “bars”), as a numeral from 0 to 5. Status follows Status property above.
- **Roam**
Whether or not the connected cell is in-network. Status follows Status property above.
- **On-Demand Ppp Enabled**
Either true or false. Reflects the platform configuration as shown in the “Provider” section of the Gprs Modem Configuration view. See “Key Properties: Provider Configuration” on page 5.
- **IP**
IP address of this JACE via the Service Provider’s VPN network, providing PPP is active. If PPP is not active, this is an empty string (with status following Status property above).
- **Imsi**
International Mobile Subscriber Identity. Unique identity for this cellular device, incorporating the SIM card identity.
- **Imei**
International Mobile Equipment Identity. Unique ID for the actual GPRS modem device, reflecting a code incorporating the modem manufacturer and model.
- **Sim**
SIM, or Subscriber Identity Module. Unique ID of the SIM card installed in the GPRS modem.

SMS application for GPRS

The GPRS modem option also enables a JACE station to send SMS (Simple Message Service, or Short Message Service) text messages to other cellular devices (cell phones), such as alarms, events, or even prepared “general use” text messages.

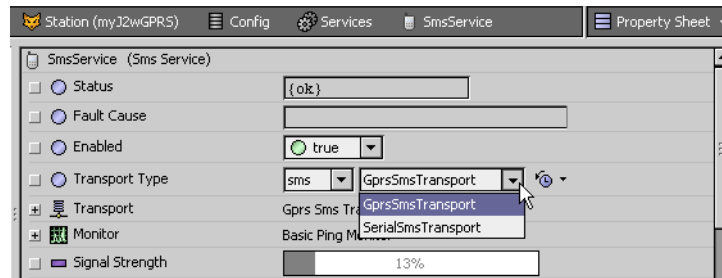
Note: For this, the JACE requires the “sms” feature in its license, the “sms” module installed, and the SmsService in its station's Services folder. Also, configured SmsRecipient and/or Sms components are needed in the station to route or configure text messages. For more details, see the NiagaraAX SMS Users Guide.

This typical outbound usage of the GPRS modem option is relatively simple, and uses the service provider's "SMSC" (Short Message Service Center, or Short Message Center) for "store and forward" of sent text messages. Note that while alarms routed via SMS are received on cell phones, currently there is no provision for alarm acknowledgment back to the JACE using SMS.

Note: *The JACE station can also receive SMS messages through the SmsService. However, apart from received SMS commands (see ["Remote SMS commands"](#)), this requires a custom Program object or component, linked to the "received" topic slot on the SmsService. This subject is outside the scope of this document.*

In the property sheet view of the JACE station's SmsService, ensure that the "Transport Type" is set to "GprsSmsTransport" to utilize the GPRS modem option. See [Figure 12](#) below.

Figure 12 *GprsSmsTransport must be selected in station's SmsService*



Remote SMS commands

The GPRS modem option has the ability to react to a small set of well-defined SMS messages that can be sent from a remote cell phone or other SMS agent.

The syntax of such a command is simple:

- the message must begin with the text "gprsd:"
- and must contain a valid command after the ":"

See the sections ["Related configuration items"](#) and ["Available remote SMS commands"](#) for more details.

Related configuration items

The following GPRS modem configuration items affect usage of remote SMS commands:

- "Enable Remote SMS Commands" must be enabled. See ["SMS Configuration"](#) on page 13.
- "Monitor data poll cycle time" determines the interval that the driver reads SMS messages as part of the "monitor data poll cycle." See ["Modem Configuration"](#) on page 12.

Available remote SMS commands

The following SMS commands can be issued remotely:

- **gprsd:pppon**
Causes a startup of the ppp protocol stack, if not already started (otherwise, this command does nothing). Note this is irrespective of the setting for the "enable ppp on ASC0" configuration item.
- **gprsd:pppoff**
Causes any current ppp session to terminate. If there is no current ppp stack initialized, this command does nothing. Note that the ppp stack cannot be restarted again until the "min time before re-connecting ppp" has transpired.
- **gprsd:sendip**
Causes the driver to return the current IP address associated with the current ppp session back to the sender's phone number. In this manner, a mobile phone can request the IP address, get an answer, and then that IP address can be used to sent up a client session (i.e. Workbench) with the JACE.
- **gprsd:info**
Causes an SMS message that contains mostly a subset of the runtime monitor data to be sent back to the sender's phone number. This data includes the following:
 - model
 - host ID of the JACE (note that this item is *not* part of the runtime data)
 - connectedLocalIpAddress
 - engineState
 - rssi
 - roam

GPRS modem LEDs

There are two LEDs on the GPRS modem option card:

- [Status LED](#)
- [Signal LED](#)

Note: The M2M JACE has only the [Status LED](#), visible on the front left cover (bottom-most LED: “GPRS”).

Status LED

The Status LED flashes in various patterns, based on the state of the modem. This LED is tied to the modem’s hardware SYNC pin, and is therefore directly under control of the modem itself (rather than the modem driver). The SYNC pin functionality is configured by sending the “AT^SSYNC=1” command during modem initialization, at driver startup.

The following LED patterns shown in [Table 1](#) are possible, (taken from the document TC63 AT Command Set, table 19.1).

Table 1 Status LED behavior for GPRS modem option

Status LED pattern	ME operating status if AT^SSYNC=1
Permanently Off	ME is one of the following modes: <ul style="list-style-type: none">• POWER DOWN mode• AIRPLANE mode• CHARGE ONLY mode• NON-CYCLIC SLEEP mode with no temporary wake-up event in progress
600ms On / 600ms Off	Limited Network Service: Either no SIM card inserted or no PIN entered, or network search in progress, or ongoing user authentication, or network login in progress.
75ms On / 3sec Off	IDLE mode: The mobile is registered to the GSM network (monitoring control channels and user interactions). No call is in progress.
75ms On / 75ms Off / 75ms On / 3sec Off	One of more GPRS PDP contexts activated.
500ms On / 50ms Off	Packet switched data transfer is in progress.
Permanently On	Depending on type of call: <ul style="list-style-type: none">• Voice call: Connected to remote party.• Data call: Connected to remote party or exchange of parameters while setting up or disconnecting a call.

Signal LED

The Signal LED on the GPRS modem card is used to indicate the RSSI (received signal strength indicator) as reported by the “AT^SIND?” command (refer to the *TC63 AT Command Set* document). This command is sent periodically to the modem from the driver at a frequency determined by the configuration parameter “Monitor data poll cycle time”, and is thus dependant on “Enable poll for monitor data” being enabled (see “[Modem Configuration](#)” on page 12).

[Table 2](#) shows the Signal LED patterns that are possible.

Table 2 Signal LED behavior on GPRS modem option card

Signal LED pattern	Pattern details	Meaning
On / Off continuous	1 sec On / 1 sec Off	Signal level not determined. Possible causes are: <ul style="list-style-type: none">• the AT^SIND? returned an error.• the configuration parameter “Enable poll for monitor” is set to false.
Off, no flashes	always Off	RSSI is 0 (<-112 dbm) or modem driver failed or not started.
1 short flash	350ms On / 2 sec Off	RSSI is 1 (-112 dbm to -97 dbm).
2 short flashes	350ms On / 350ms Off / 350ms On / 2 sec Off	RSSI is 2 (-97 dbm to -82 dbm).

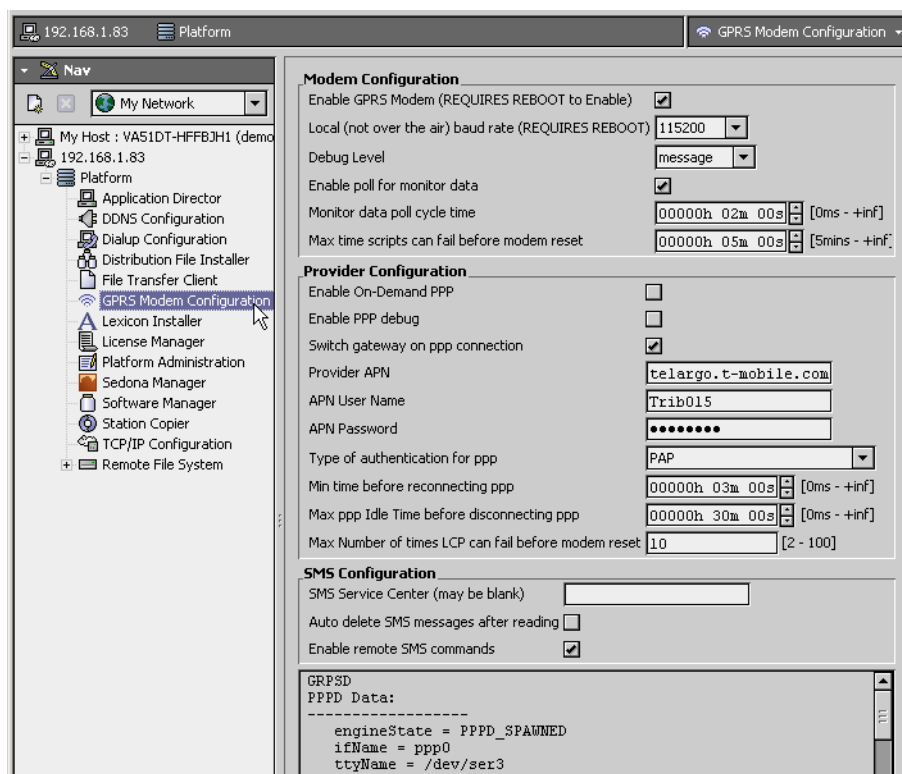
Signal LED pattern	Pattern details	Meaning
3 short flashes	350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 2 sec Off	RSSI is 3 (-82 dbm to -67 dbm).
4 short flashes	350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 2 sec Off	RSSI is 4 (-67 dbm to -52 dbm).
5 short flashes	350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 350ms Off / 350ms On / 2 sec Off	RSSI is 5 (> -52 dbm).

GPRS Modem Configuration view

Reference

The GPRS Modem Configuration view (Figure 13) is one of several platform views for a QNX-based JACE, when using AX-3.4 Workbench or later. It is used to configure the (wireless) GPRS modem option that may be installed in the host JACE controller.

Figure 13 GPRS Modem Configuration view



In order to operate, the GPRS modem option must have a [SIM](#) card (Subscriber Identity Module) installed. The SIM card must be from an approved [Service Provider](#).

Note: Associated with this, several key properties must be entered in the configuration sections of this view. See the previous section “[Required platform GPRS setup](#)” on page 5 for details.

The following sections provide additional reference details about this platform view:

- [GPRS modem configuration sections](#)
- [Runtime data area](#)
- [GPRS modem LEDs](#)
- [Remote SMS commands](#)

GPRS modem configuration sections

As shown in [Figure 13](#), the [GPRS Modem Configuration view](#) has the following configuration sections:

- [Modem Configuration](#)
- [Provider Configuration](#)
- [SMS Configuration](#)

In addition, a [Runtime data area](#) near the bottom of the view shows data served up from modem.

Modem Configuration

This section of the platform [GPRS Modem Configuration view](#) includes the following properties:

- **Local (not over the air) baud rate**
With drop-down menu selections from 460800 baud to 9600 baud. This is the baud rate at which the JACE comm port talks to the GPRS modem. *It is not representative of the actual data throughput of the GPRS modem*, that is, this is *not* the “over the air” baud rate. Note that:
 - Takes effect only after a reboot.
 - Defaults to 115200 baud, which matches factory default rate of the GPRS modem. In general, the fastest rate supported by the modem is best.
- **Set Debug Level**
To specify how much information is sent to the serial shell console output (the JACE’s “system shell” jumper must be installed), with choices trace, message (default), warning, error. Any change takes effect immediately.
- **Enable poll for monitor data**
This allows the monitor thread to poll the modem’s second port (ASC1) independently of any traffic (that is, ppp) on the primary modem port (ASC0). Data polled includes items in the “[Monitor Data](#)” section of the bottom-most runtime data area of this view. Any change takes effect immediately.
Note: Monitor polling data includes signal strength, which is used to flash the “Signal LED” on the GPRS modem option card. Therefore, if this property is disabled (cleared), the Signal LED will flash a 1 sec. On / 1 sec. Off pattern to indicate the signal level is not being read.
- **Monitor data poll cycle time**
Specifies how often the low-level modem driver polls for data in the “[Monitor Data](#)” section of the bottom-most runtime data area. Any change takes effect upon timeout of the previous monitor.
- **Max time scripts can fail before modem reset**
Specifies the duration that “modem quite time exceeded” from scripts (monitor thread) failure can occur before a modem restart is attempted using the AT^SMSO shutdown command. Range is from 5min. (default) to any greater time.

Provider Configuration

This section of the [GPRS Modem Configuration view](#) is to specify the cellular provider (corresponding to the SIM card installed in the GPRS modem option), along with numerous properties related to the PPP (point-to-point) protocol used for GPRS connections.

Provider configuration properties include:

Note: *Changes to any of the first three (checkbox) properties become effective as follows:*

- If changed while a ppp session is not already active, the change is effective immediately (and a ppp session is attempted immediately).
- If changed while a ppp session is already active, it takes effect on the next ppp session (current ppp session must end first). The current ppp session normally ends on “Max ppp Idle Time before disconnecting ppp”.
- **Enable On-Demand PPP**
(Checkbox) Determines how and when the ppp protocol stack is initialized by the driver software.
 - If disabled (cleared), then an attempt to start the ppp stack is performed shortly after JACE boot. Consider this the “always on” usage of ppp. The items “Min time before reconnecting ppp” and “Max ppp Idle Time before disconnecting ppp” both come into play in this mode.
 - If enabled (checked), then the ppp stack is initialized only “on demand” whenever the IP stack requires communications, and a route does not already exist to the destination. Consider this the “autoconnect” mode of operation. The property “Max ppp Idle Time before disconnecting ppp” is used, but the property “Min time before reconnecting ppp” is ignored in this mode.
- **Enable PPP debug**
(Checkbox) Enables the ppp stack to send detailed information to the serial console of the JACE. This can be useful to troubleshoot when ppp parameter negotiation or authentication fails.

- **Switch gateway on ppp connection**
(Checkbox) After successful initialization and connection of the ppp stack, typically the ppp server will have assigned a gateway address to use for the IP stack. If enabled, this property will cause the original gateway configured in the JACE's TCP/IP configuration to be temporarily "swapped out" with the gateway assigned during the ppp client/server negotiation. This allows connectivity to IP addresses that are on the ppp subnet.
- **Provider APN**
The Access Point Name for the cellular provider network. The APN specifies the gateway between the mobile network and the Internet.
- **APN User Name**
User name used to authenticate to the provider network.
- **APN Password**
Password used to authenticate to the provider network.
- **Type of authentication for ppp**
Used to set the authentication type for the ppp session, where choices are:
 - **none**
No authentication
 - **PAP**
(Password Authentication Protocol), where in most cases, either this or CHAP is acceptable.
 - **CHAP**
(Challenge Authentication Handshake Protocol), where in most cases this or PAP is acceptable.
 - **MS-CHAP-V1, CHAP, PAP**
(some combination of Microsoft's version 1 of CHAP, CHAP, or PAP).
- **Min time before reconnecting ppp**
This specifies a timer timeout that is enforced whenever a ppp session terminates for any reason. This is the time that the ppp stack will remain deactivated before any attempt to restart can be initiated.
- **Max ppp Idle Time before disconnecting ppp**
Once the ppp session has been started, inactivity on the link for this amount of time will cause the ppp session to terminate. Default value is 30 minutes.
- **Max Number of times LCP can fail before modem reset**
Specifies the number of unsuccessful LCP (Link Control Protocol) requests by the pppd before the the AT^SMSO command is sent to reset the modem. Default value is 10, range is from 2 to 100.

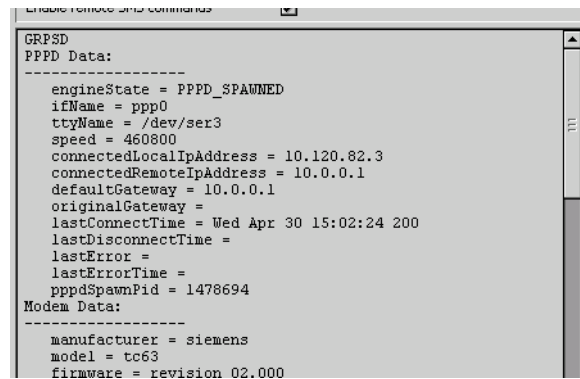
SMS Configuration

This section of the [GPRS Modem Configuration view](#) defines the behavior of the SMS (Short Message Service) handling portion of the GPRS modem driver. Properties include:


- **SMS Service Center (may be blank)**
Specifies the phone number of the SMS service center. Depending on provider, this may be preset in the SIM card in the GPRS modem, and so may be blank. Any change takes effect immediately.
- **Auto delete messages after reading**
If enabled (checked), messages marked as "REC_READ" are deleted. Messages are marked "REC_READ" if they are read by external agents (such as the SMS platform service). Also, if the SMS message is marked as "REC_UNREAD" and it is a special "remote command" type of message, it is also deleted, regardless of this setting.
- **Enable remote SMS commands**
If enabled (checked), this allows the processing of special SMS "commands" that were sent remotely. See ["Remote SMS commands"](#) on page 9.

Runtime data area

The bottom area of the [GPRS Modem Configuration view](#) (Figure 14) contains data from the low-level GPRS modem driver ("GPRSD") on the JACE.

Figure 14 Runtime data area near bottom of GPRS Modem Configuration view

```
Enable Remote SMS Commands
GPRS
PPPD Data:
-----
engineState = PPPD_SPAWNED
ifName = ppp0
ttyName = /dev/ser3
speed = 460800
connectedLocalIpAddress = 10.120.82.3
connectedRemoteIpAddress = 10.0.0.1
defaultGateway = 10.0.0.1
originalGateway =
lastConnectTime = Wed Apr 30 15:02:24 200
lastDisconnectTime =
lastError =
lastErrorTime =
pppdSpawnPid = 1478694
Modem Data:
-----
manufacturer = Siemens
model = tc63
firmware = revision 02.000
```

This information updates only when you load or refresh  this view. Runtime data appears divided in the following sections:

- [PPPD Data](#)
- [Modem Data](#)
- [SMS Data](#)
- [Monitor Data](#)

PPPD Data

This section in the [Runtime data area](#) shows “ppp” (point to point protocol) related data, including the following:

- **engineState**
Current state of the pppd control engine, as one of the following:
 - UNMOUNTED — a transitional state that should occur only when the driver starts. If it remains in this state, then the binaries necessary to run the pppd stack could not be loaded. When binaries successfully load, this state changes to INITIALIZING MODEM.
 - INITIALIZING MODEM — AT commands are being sent to the modem in order to set it up for GPRS connection over port ASC0. If successful, the state changes to STOPPED.
 - STOPPED — modem has been initialized successfully, and is ready to connect. This is the normal state for the engine in cases where “Enable use of ppp on ASC0” is set to false, else this is a transitional state if that [Provider Configuration](#) property is true. If conditions allow a connection, then AT commands are set to the modem to attach to the GPRS provider network, upon which the state transitions to CONNECTED.
 - CONNECTED — modem has successfully connected to the GPRS network, and is attempting to initialize the ppp stack. If successful, the state transitions to PPPD_SPAWNED.
 - PPPD_SPAWNED — The ppp stack has been loaded and initialized with successful negotiation of the LCP parameters, and authentication to the server was performed. The ppp connection is now operational and ready to accept IP packets. This is the normal state when a ppp connection has been established.
 - DISCONNECTING — if the ppp stack detects that no packets have been transmitted within the “Max ppp idle time before disconnecting”, then the ppp stack terminates, and the engine enters this state. While in this state, AT commands are sent to hang up the GPRS connection. If successful, the state then transitions to DISCONNECTED.
 - DISCONNECTED — the pppd engine stays in this state for “Min time before reconnecting” time, upon which time the state transitions to STOPPED, and the cycle repeats.
- **ifName**
Interface name associated with the ppp stack. Will be blank until a ppp session is active.
- **ttyName**
Name of the serial interface device the ppp connection uses on the JACE. This is physically tied to ASC0 on the modem.
- **speed**
Actual baud rate the JACE’s serial interface uses to talk to the GPRS modem option’s UART.
- **connectedLocalIpAddress**
Address assigned to the ppp stack, usually set during LCP negotiation in the ppp connection process.
- **connectedRemoteIpAddress**
Address of the ppp server that is connected to.

- **nameServer(s)**
DNS servers for the connected ppp server and original (before ppp connection) gateway.
- **defaultGateway**
Gateway address that the JACE IP stack uses to forward packets. Should be the same as the connectedRemoteIpAddress if a ppp session is active, and “Switch gateway on ppp connection” is set true.
- **originalGateway**
If “Switch gateway on ppp connection” is set true, this address is the gateway in use before ppp was started. Once ppp terminates, this address is written back to the “defaultGateway” of the IP stack.
- **lastConnectTime**
Last time (local time) that a ppp session was established.
- **lastDisconnectTime**
Time of the last ppp disconnect, for any reason.
- **lastError**
Reason for last ppp termination.
- **lastErrorTime**
Time of the last error that caused ppp termination.
- **pppdSpawnPid**
Process ID in the JACE of the pppd process.
- **pppdSpawnCount**
Number of times the pppd process has spawned.
- **lcp negotiate failures**
Number of times LCP negotiations failed to complete with success.
- **modem shutoff commands**
Number of times the AT^SMSO command was sent as a result of the “Max number of times LCP can fail before modem reset” property threshold being reached. See related [Provider Configuration](#) property.

Modem Data

This section in the [Runtime data area](#) shows data about the installed GPRS modem option, including the following:

- manufacturer — the manufacturer of the installed modem, read via AT command during initialization of the modem.
- model — the installed modem’s model number.
- firmware — the installed modem’s firmware revision level.
- imei — “international mobile equipment identity”.
- imsi — “international mobile subscriber identity”.
- SIM card status — status of SIM card, such as “SIM initialization completed”.
- SIM card ID — the ID number of the installed SIM card.
- lastFailedScriptCmd / lastFailedScriptCmdResult / lastFailedScriptCmdTime — these values are set if an AT command sent to the modem returns an “error” response.
- CEER — extended error report values from the AT+CEER command. For details on interpreting this value, refer to the Siemens document TC63_ATC_V02.500 *TC63 AT Command Set*.
- optionBoardResets — number of times the modem has been reset by the AT^SMSO command.
- lastOptionBoardResetTime — time of the last reset by the AT^SMSO command.

SMS Data

This section in the [Runtime data area](#) shows data about failed SMS messages, including:

- lastFailedSmsCmd / lastFailedSmsCmdResult / lastFailedSmsCmdTime — these values are set if an SMS message fails to be sent.

Monitor Data

This section in the [Runtime data area](#) shows various data, with various following descriptions using terms ME (mobile equipment), MS (mobile station), PLMN (public land mobile network):

- **signal quality**
The estimated BER (bit error rate) on the received signal. Valid values are 0—7, with 0 as less than 0.1% BER (fewest errors) and 7 as greater than 15% BER. A 99 value means this has not been read yet.
- **registration**
If false, then not registered on any provider network, or if true and “roam” is false, then registered to home network, of if true and “roam” is true, then registered to another network.

- **roam**
If false, then registered to home network or not registered, of if true then registered to another network.
- **rsi**
Received signal strength indicator, where:
 - 0: signal strength \leq -112 dbm
 - 1—4: signal strength in 15 db steps
 - 5: signal strength \geq -51 dbm
- **sms full**
If true, sms memory space is full; if false, sms memory space is not full.
- **cons**
The “enhanced operator name string”.
- **nit**
The “network identity and time zone” information.
- **band**
Currently selected frequency band or band combination.
- **CREG:**
Network Registration Status, as one of the following:
 - 0: Not Registered — ME is currently not searching for new operator. Normally, status 0 occurs temporarily between two network phases (status 2). However, if it persists, one of the following reasons may apply:
 - If automatic network selection is active, there is probably (either) no SIM card available, no PIN entered, or no valid Home PLMN entry found on the SIM.
 - If manual network selection is active and the selected network is available, login fails due to one of the following: #11 PLMN not allowed, #12 Location area not allowed, #13 Roaming not allowed in this location area.In either case, user intervention is required. Yet, emergency call can be made if any network is available.
 - 1: Registered to home network.
 - 2: Not Registered — but ME is currently searching for a new operator. The ME searches for an available network. Failure to log in until after more than a minute may be due to one of the following reasons:
 - No network available or insufficient Rx level.
 - The ME has no access rights to the networks available.
 - Networks from the SIM list of allowed networks are around, but login fails due to one of the following: #11 PLMN not allowed, #12 Location area not allowed, #13 Roaming not allowed in this location area.After this, the search will be resumed (if automatic network search is enabled).
 - The Home PLMN or allowed PLMN is available, but login is rejected by the cell (reasons: Access Class or LAC). If at least one network is available, emergency calls can be made.
 - 3: Registration denied — Authentication or registration fails after Location Update Reject due to one of the following reasons:
 - #2...IMSI unknown at HLR.
 - #3...Illegal MS
 - #6...Illegal MEEither the SIM or the MS or the ME are unable to log into any network. No further attempt is made to search or log into a network. User intervention is required. Emergency calls can be made, if any network is available.
 - 4: Unknown (not used).
 - 5: Registered, roaming. The ME is registered at a foreign network (national or international network).
- **CCREG:**
GPRS Network Registration Status, as one of the following:
 - 0: Not Registered — ME is not currently searching an operator to register to. The ME is in GMM state GMM-NUL or GMM-DEREGISTERED-INITIATED. GPRS service is disabled, the ME is allowed to attach to GPRS if requested by the user.
 - 1: Registered to home network. The ME is in GMM state GMM-REGISTERED or GMM-ROUTING-AREA-UPDATING_INITIATED on the home PLMN.
 - 2: Not Registered — But ME is currently trying to attach or searching an operator to register to. The ME is in GMM state GMM-DEREGISTERED or GMM-REGISTERED-INITIATED. The GPRS service is enabled, but an allowable PLMN is currently not available. The ME will start a GPRS attach as soon as an allowable PLMN is available.

- 3: Registration denied — The ME is in GMM state GMM-NULL. The GPRS service is disabled, the ME is not allowed to attach to GPRS if requested by the user.
- 4: Unknown
- 5: Registered, roaming — The ME is in GMM state GMM-REGISTERED or GMM-ROUTING-AREA-UPDATING-INITIATED on a visited PLMN.
- MONI**
Monitor idle mode and dedicated mode. See section 8.9.1 in the Siemens document *TC63 AT Command Set* for full explanations of fields in this entry.
- SMONG**
GPRS Monitor, supplies GPRS specific cell information.

Column	Description
BCCH	ARFCN of BCCH carrier
G	GPRS status, where: 0 = not available in currently used cell, 1 = available in currently used cell, 2 = GPRS attached <i>Note: If the network uses the PBCCH, the correct value can only be displayed if the TC63 is attached.</i>
PBCCH	If PBCCH is present, indication of ARFCN, else “-” or if Frequency hopping is used, “H”.
PAT	Priority Access Threshold (GSM Rec. 04.08 / 10.5.2.37b), where: <ul style="list-style-type: none"> 0 — Packet access is not allowed in cell. 1 — Spare, shall be interpreted as “000” (packet access not allowed). 2 — Spare, shall be interpreted as “000” (packet access not allowed). 3 — Packet access is allowed for priority level 1. 4 — Packet access is allowed for priority level 1 to 2.
MCC	Mobile Country Code
MNC	Mobile Network Code
NOM	Network Operation Mode (1...3)
TA	Timing Advance Value
RAC	Routing Area Code (as hexadecimal value)

- modem voltage**
Modem supply voltage as measured by the GPRS modem.

Document change log

Updates (changes/additions) to this *NiagaraAX GPRS Modem Option - Engineering Notes* document are listed below.

- Updated: June 7, 2010
Mostly minor changes. Added notes in the [SIM](#) card section and a configuration section (“[Key Properties: Provider Configuration](#)” on page 5) about needing a username and password from the service provider. Removed references to Fox and HTTP tunneling through a JACE that was erroneously included in some “use case” figures—such tunneling is available only on a AxSupervisor platform. Added a new section “[TCP/IP configuration with GPRS modem](#)” on page 7 that explains DNS servers should *not* be configured, *nor* DHCP used, on any JACE using a GPRS modem.
- Updated: January 21, 2009
Minor changes, noting new “M2M JACE” platform in several places. This JACE is available with an onboard GPRS modem option, equivalent to the GPRS modem option card for other JACEs. Added descriptions for two new GPRS modem properties found in the “[GPRS Modem Configuration view](#)” on page 11, including one new [Modem Configuration](#) property and one new [Provider Configuration](#) property (each the last one listed), as well as a few new entries in the [Runtime data area](#) of that view. All relate to a “modem restart” routine implemented for a rare intermittent issue. Included also is a note in the section “[SMS application for GPRS](#)” on page 8 that explains that the station’s SmsService can also receive SMS messages. Typos in remote SMS commands were corrected in “[Remote SMS commands](#)” on page 9.
- Updated: October 3, 2008
Minor changes, including a repeated Note in the section “[Use cases for GPRS equipped JACEs](#)” on page 2 that explains GPRS connection speeds are similar to that for dialup modems. Two empty “usage notes” sections were also removed in the appendix “[Wyless as service provider](#)”.
- Publication: September 16, 2008
Initial “Engineering Notes” type document.

Wyless as service provider

Note: At the time of this document it is not known if other wireless Service Providers (apart from Wyless) use the same type of VPN (Virtual Private Network) architecture and connectivity techniques described in this section. Therefore, this information was organized in this appendix where Wyless is assumed to be the Service Provider. Future revisions of this document may provide details specific to other, different, wireless Service Providers—as this information becomes known.

The following main sections currently apply:

- “GPRS connectivity overview” on page 18
- “Connecting as a VPN client to a JACE with GPRS modem option” on page 19
- “Configuring an IPSec VPN gateway to access a VPN network” on page 21

GPRS connectivity overview

Wireless Internet connectivity to a JACE controller is available starting in AX-3.4, using the GPRS cellular modem option and a VPN (Virtual Private Network) connection. Typical usage is where an ISP (Internet Service Provider) may not be available in the area, or possibly the local IT department does not want the NiagaraAX system on the local LAN. Or, for remote monitoring of a site where relatively few data points are collected, and where the cost of obtaining a permanent broadband connection is regarded as too high.

The following sections provide an overview of two main applications of the GPRS modem option:

- Normal connectivity to a JACE, that is using Workbench (Fox or platform), a web browser, or by another station (AxSupervisor). See the next section “GPRS connectivity options”.
- Outbound annunciation of alarms or other messages to other cell phones as “short message text” (SMS) messages. See “SMS application for GPRS” on page 8.

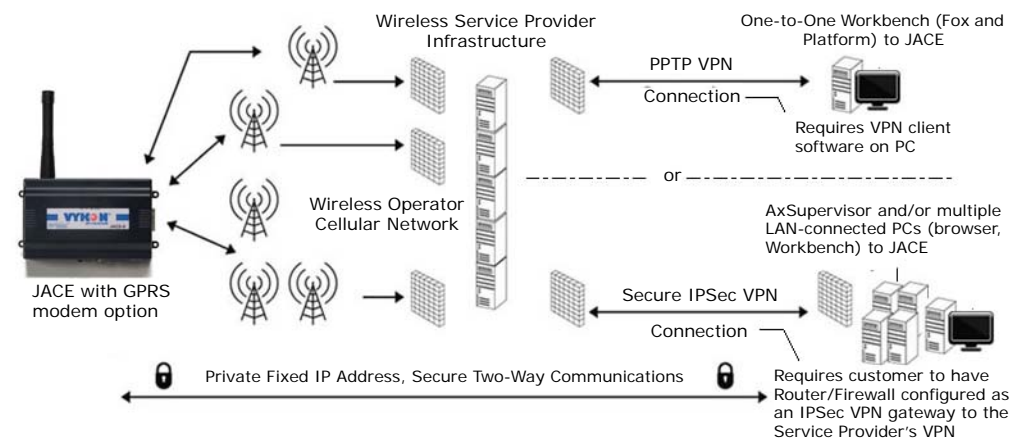
Depending on configuration, both applications of a GPRS modem-equipped JACE may be used.

GPRS connectivity options

As shown in Figure 15, there are two (2) different ways of connecting to a remote JACE using the GPRS modem option: a PPTP connection, or through an IPSec VPN gateway.

Note: GPRS connection speeds are similar to dialup modems—typically 30 - 60Kbps download, and 10 - 15Kbps upload. Therefore, JACE operations such as software upgrades are not recommended. Instead, a direct connection (to LAN1 or LAN2 port of the JACE) should be used when a large transfer of data is needed.

Figure 15 Remote connectivity to GPRS modem-equipped JACE using either PPTP or IPSec techniques



PPTP connection to GPRS modem

A PPTP (Point-to-Point Tunnel Protocol) VPN connection to the JACE is best suited for a “one-to-one” connection over the Internet between the JACE and a single user, typically either Workbench (Fox or platform) or a web browser. It is intended for temporary access to the JACE for monitoring purposes, such as by the end-user with a browser, or to perform light engineering using Workbench.

The PC accessing the JACE must use VPN client software. Typically, on a Windows PC you use a “Virtual Private Network” object created within Window’s “Network Connections”, then configure it with connection data furnished by the Service Provider. After starting this VPN connection, you can then open the JACE station or platform in Workbench, or if needed access it in a web browser.

For more details, see [“Connecting as a VPN client to a JACE with GPRS modem option”](#) on page 19.

IPSec VPN gateway to GPRS modem

An IPSec VPN gateway connection is a more robust technique, and is recommended for AxSupervisor connectivity to any remote JACE via its GPRS modem option. Also, this method can allow a customer’s entire LAN access to the Service Provider’s VPN network with the GPRS modem-equipped JACEs. It also offers higher total bandwidth and supports simultaneous connections to multiple JACEs. In addition, IPSec provides better reliability and error-recovery than a PPTP connection. VPN client software is not required or used.

To employ, the customer must provide and install a suitable VPN router/firewall, and configure it in co-operation with the Service Provider. This device acts as the customer-side of a “IPSec tunnel” to the Service Provider, connected to another VPN gateway device on the provider’s side.

Typically, configuration requires the customer’s IT department to work closely with Service Provider, and specific details may vary from one implementation to the next. For details specific to an example setup with the Wyleless network service provider, see [“Configuring an IPSec VPN gateway to access a VPN network”](#) on page 21.

Connecting as a VPN client to a JACE with GPRS modem option

After the necessary platform configuration of any JACE with GPRS modem option (see [“Required platform GPRS setup”](#) on page 5), you should be able to use a VPN connection to establish PPTP communications to that JACE over the Internet.

The following procedures explain how to create a VPN connection object on your PC using Windows, for which you configure with parameters supplied by your [Service Provider](#).

- [Creating a Windows VPN connection object](#)
- [Setting the proper gateway operation for the VPN client](#)

Creating a Windows VPN connection object

At your Windows PC, do the following:

- Step 1 Open the Windows Control Panel (click **Start > Control Panel**).
Among the control panel objects is one for **Network Connections**.
- Step 2 Double-click **Network Connections**.
Your network connection objects appear, including a link for a **New Connection Wizard**.
- Step 3 Double-click the **New Connection Wizard**.
The “New Connection Wizard” welcome dialog appears. Click **Next** to continue.
- Step 4 In the “Network Connection Type” step, there are several available choices.
Select “Connect to the network at my workplace”, and click **Next** to continue.
- Step 5 In the “Network Connection” step, there are two choices (Dial-up or Virtual Private Network).
Select “Virtual Private Network Connection”, and click **Next** to continue.
- Step 6 In the “Connection Name” step, enter a name that is meaningful to you (name does not affect operation, and you can change this later if desired). For example, type in Wyleless VPN
Click **Next** to continue.
- Step 7 In the “Public Network” step, select “Do not dial the initial connection”, and click **Next** to continue.
- Step 8 In the “VPN Server Selection” step, enter the VPN server name or address furnished by your Service Provider. For example for Wyleless, you enter: vpn.wyleless.net
Click **Next** to continue.
- Step 9 If a “Smart Card” step appears, choose No (“Do not use my smart card”), and click **Next** to continue.
- Step 10 In “Connection Availability” step, you typically select “Anyone’s use”. Click **Next** to continue to the “Completing the New Connection Wizard” dialog.

- Step 11 In the “Completing the New Connection Wizard” dialog, choose whether a desktop shortcut should be added for this connection, and click **Finish**.
The “Connect *ConnectionName*” popup dialog appears (e.g. “Connect Wyless VPN”), with fields for credentials (User name and Password), as well as save options for these credentials. See [Figure 16](#).

Figure 16 Connect *ConnectionName* dialog



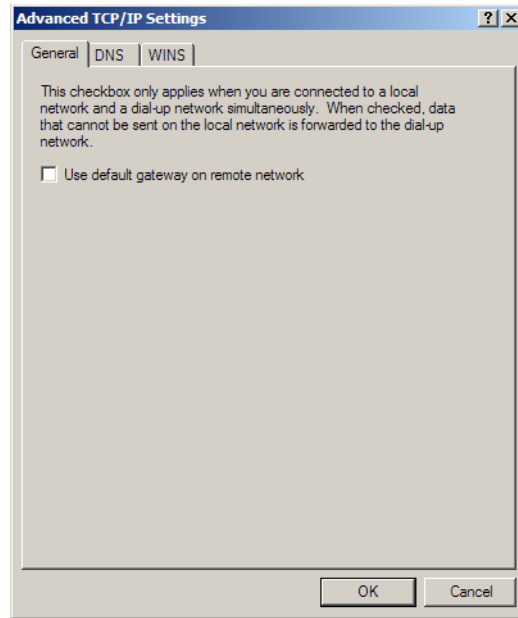
- Step 12 In the “Connect *ConnectionName*” dialog, enter the VPN access user name and password as furnished by your Service Provider.
Typically, you also check (enable) the “Save the user name and password for the following users”, selecting either “Me only” or “Anyone who uses this computer”.
- Note:** *Do not **Connect** yet! An important setting must be configured in the **Properties** of this object first! See the next procedure, “[Setting the proper gateway operation for the VPN client](#)”.*

Setting the proper gateway operation for the VPN client

With the “Connect *ConnectionName*” dialog open for the newly-created VPN client connection object (as shown in the previous [Figure 16](#)):

- Step 1 Click the **Properties** button.
A multi-tabbed dialog appears. Select the **Networking** tab.
- Step 2 In the **Networking** tab, click to highlight the listed “Internet Protocol (TCP/IP)” item, and then click the **Properties** button.
An “Internet Protocol (TCP/IP) Properties” dialog appears with a single “General” tab, including an **Advanced...** button.
- Step 3 Click the **Advanced...** button.
The “Advanced TCP/IP Settings” dialog appears, with a “General” tab.
- Step 4 In the “General” tab of the “Advanced TCP/IP Settings” dialog, *make sure the checkbox is cleared for:*
Use default gateway on remote network (see [Figure 17](#)).

Figure 17 Clear option to “Use default gateway on remote network” in Advanced TCP/IP Settings dialog



Note: This is necessary to prevent forwarding of all TCP/IP traffic from your PC to the remote VPN network, which can overload the Service Provider and cause various connection issues.

Step 5 Click **OK** in each opened dialog to close and save.

The “Connect ConnectionName” dialog (Figure 16) remains. Click the **Connect** button to connect. While connected, you see a “connected” state by the network connection object in your **Network Connections** folder.

Note: Once connected, you can use Workbench to connect to a GPRS modem-equipped JACE using its Service Provider assigned static IP address, either to open its station (Fox) or a platform connection. Or, use a browser connection to the station if it is running the Webservice.

Configuring an IPSec VPN gateway to access a VPN network

This section explains configuring a persistent IPSec tunnel connection (gateway) to one or more subnets on a Service Provider’s VPN network. For an overview, see “[GPRS connectivity options](#)” on page 18. This IPSec VPN gateway provides a transparent, secure, network layer between hosts on the customer’s network and GPRS modem equipped-JACEs on the [Service Provider’s](#) network.

Note: This is an advanced topic. It is recommended that configuration be done only by a knowledgeable IT professional working in cooperation with the Service Provider. Note that this section ends with a configuration example using Wyless as the Service Provider, and is specific to one piece of hardware (a Linksys RVL200 router) configured as the IPSec VPN gateway.

NAT transversal (Network Address Translation) is beyond the scope of this document.

The following main sections are included:

- [IPSec gateway configuration overview](#)
- [Provisioning request to Service Provider](#)
- [Linksys RVL200 as IPSec VPN gateway to Wyless example](#)

IPSec gateway configuration overview

A customer’s business network has some number of hosts (often PCs) that typically include one or more AxSupervisors, often which need to communicate with GPRS modem-equipped JACEs. This network is managed by the customer’s IT department, and typically includes some combination of devices and software such as routers, firewall, and a gateway to the Internet.

To best integrate the external VPN network (with JACEs) into the customer’s network, *another* dedicated device (router or firewall) must be placed on the customer’s network, and configured to act as a client “tunnel connection”, or gateway, to this “server network.”

Note: Selection advice for the customer’s IPSec VPN gateway device is beyond the scope of this document. However, Tridium configured and used a Linksys RVL200 router, a relatively inexpensive device.

The IPSec VPN gateway negates the need for “VPN client software” on any of the customer’s hosts—as would be required for any PPTP (one-to-one) connection. Instead, this gateway automatically links the customer’s designated IP subnet to the remote subnet(s) of the Service Provider’s VPN network.

This “tunnel connection” uses IPSec (IP Security Architecture) associations, as configured on both “sides” of the tunnel. IPSec associations include various security parameters such as algorithms and keys. These parameters must be selected and known on both sides of the tunnel—meaning both to the customer and to the Service Provider.

To do this, upon customer request, a Service Provider sends the customer a “VPN provisioning form” that identifies the IP address, machine type, and protocol(s) used on the firewall/VPN gateway on *their side* of the connection, along with at technical contact for VPN provisioning. The customer then completes other areas of the form, selecting among various types of IPSec parameters. Also, the customer identifies the machine type of their dedicated gateway device, along with its static, public IP address, and technical contact information. For more details, see the next section [“Provisioning request to Service Provider”](#).

The customer submits this completed form back to the Service Provider. Following this exchange of information, an IP address range within the Service Provider’s VPN network is provisioned (made available) to the customer’s network. Any subsequent configuration information is supplied back to the customer. After the customer completes the configuration of their IPSec VPN gateway, the GPRS modem equipped JACEs should be able to communicate as if they were on the customer’s own subnet, securely.

Provisioning request to Service Provider

1. The customer contacts their Service Provider to request connection provisioning, and obtain configuration information. At this time, the customer may already have the IPSec VPN capable device they will be using as their dedicated VPN gateway, or they may wait to review the available IPSec VPN parameters needed for access.
2. The Service Provider sends the customer a “VPN provisioning form” that identifies their technical contact name, address, and phone number, along with the equipment parameters on their side. Included will be subnets being made available to the customer, along with available selections for IPSec VPN parameters (a preferred “default set” of parameters may be suggested, and are recommended). Also on this form the customer supplies their credential for authentication, as either a pre-shared key or certificate. Finally, the customer specifies equipment parameters for their side of the VPN tunnel (the IPSec VPN gateway device). For example areas of such a form (Wyless), see [“Service Provider’s \(Wyless\) Customer VPN Information”](#).
3. After the customer submits the form back to the Service Provider (information exchanged), the parties responsible for provisioning negotiate an IP range within the Service Provider’s subnet to be used to address the customer’s hosts (GPRS modem-equipped JACEs). It may be requested that one of the IP addresses be available for testing purposes—that is, always connected and “pingable”.

Service Provider’s (Wyless) Customer VPN Information

Service Provider Details	
Name, Site Address, City, Country, Technical Contact, Site Telephone	Wyless PLC, Harman House, 1 George Street, Ukbridge, UK, <i>ContactName, TelephoneNumber</i>

Customer Details	
Customer Name, Primary Site Address, City, Country, Site Contact, Technical Contact, Site Telephone Number	Tridium, 3951 Westerre Parkway, Richmond VA, USA, <i>Site-ContactName, TechnicalContactName, TelephoneNumber</i>

Wyless Firewall/VPN Gateway Details	
Firewall/VPN Gateway Make and Model	Cisco PIX 515E
VPN Protocol	IPSec
VPN Termination Address	<i>provider’s public IP address</i>

Mobile Device IP Adress/Subnets	
Subnet One	10.120.82.0/24
Subnet Two	10.117.0.0/22 255.255.252.0
Subnet Three	

VPN Parameters	
(* Notes information furnished by customer. Wyless-preferred VPN parameters are in [brackets].)	
* Customer Firewall/VPN Gateway Make and Model	Linksys RVL200
ISAKMP Encryption (select)	<ul style="list-style-type: none"> • AES • DES • [3DES] • Other
* Pre-Shared Key ^a	<i>textString</i>
* Customer VPN Termination IP Address	<i>IPaddress</i> (public, static IP address for the gateway node)
Diffie-Hellman Group (select)	<ul style="list-style-type: none"> • 1 • [2] • 3
IKE Hash (select)	<ul style="list-style-type: none"> • [MD5] • SHA
* IKE Lifetime	86400
IPSec Transform Set (select)	<ul style="list-style-type: none"> • ESP-SHA-Hmac • [ESP-3DES]
* Internal IP address range ^b	10.11.90.0/24 //negotiated
* Pingable Test Host on LAN ^c	10.11.90.250 //negotiated

- Pre-shared key to be used to establish identity before each communications session. Certificates acquired from a trusted authority can replace the use of a pre-shared key.
- Range of IP addresses local to Wyless available to be assigned to hosts from customer's network.
- Customer's host functioning as a pingable server to the client network, that Wyless can contact for testing purposes.

In the example form above, Tridium verified a proof-of-concept configuration using the following parameters: 3DES, ISAKMP over IKE, a pre-shared key (not revealed), a Diffie-Hellman group of 2, MD5 hash function, and ESP-3DES for the IPSec transformation set. The tunnel connection was established between a Cisco PIX 515E (Wyless) and a Cisco PIX 506 (Tridium).

Linksys RVL200 as IPSec VPN gateway to Wyless example

The following steps reflect configuration of a Linksys model RVL200 to provide a persistent IPSec VPN connection to Wyless over an IPSec router. Any additional provisioning that may be required for NAT-Transversal is beyond the scope of this document.

Note: Please note the following:

- The Linksys RVL200 can connect no more than two subnets to each other.
- It is presumed that the Linksys RVL200 router is started in its factory default configuration.
- Also presumed is that VPN parameters have already been selected and negotiated with Wyless, via their VPN provisioning form. See the previous section ["Provisioning request to Service Provider"](#).

The following main steps are performed:

Log into configuration page

Use an Ethernet cable connected from your PC to any of the four adjacent ports on the side of the Linksys RVL200 router. Open a web browser and navigate to the following IP address:

`http://192.168.1.1/default`

You should be prompted for login name and password (if not, check that your PC has a 192.168.1.*nnn* static IP address, the Ethernet cable is a crossover type, and the router is set to its default configuration).

The factory default login credentials for this Linksys model are "admin" for user name and "admin" for the password. After you login, you need to configure the device IP address to an address within the subnet agreed upon with Wyless.

Configure device IP address

From the Linksys router's configuration menu, navigate to **Setup > Network** to review the current LAN settings

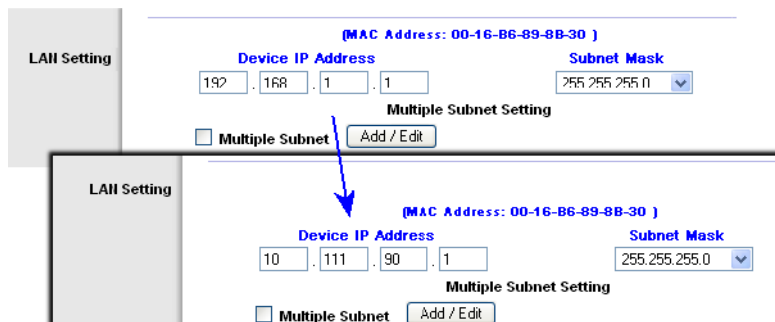
Figure 18 Linksys RVL200 Setup, Network menu



If the default IP address, 192.168.1.1 is not on the subnet as agreed upon with Wyless in their VPN form, the device's IP will need to be changed to an IP on that subnet.

Consider the "internal IP subnet" is to be 10.111.90.0/24. The default configuration is changed to look as shown in [Figure 19](#) below.

Figure 19 LAN Setting default re-configured to be on internal IP subnet



Note in this case the subnet mask is not changed, only because the internal subnet mask is a 24-bit mask by default, and need not change.

The VPN parameters may not explicitly state an IP address to use as the IPSec router's IP address. In this case you can choose an address from any available IP address.

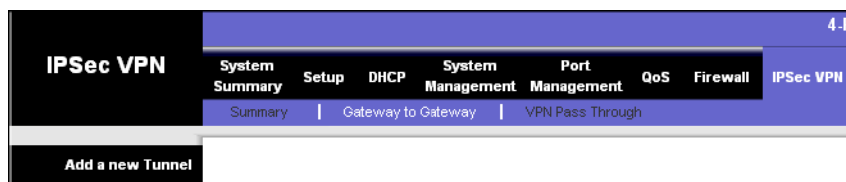
After changing the Linksys router's Device IP Address, save the change by clicking the "Save Settings" link on the bottom right of the page.

Note: This new IP address is immediately effective after saving. Therefore, it is necessary to navigate to this new IP address in your web browser, and login again.

Create and configure the IPSec tunnel

After login to the Linksys RVL200 router from a browser, navigate to the **IPSec VPN > Gateway to Gateway** page. Choose to "Add a new Tunnel", as shown in [Figure 20](#) below.

Figure 20 IPSec VPN menu item Add a new Tunnel (Linksys RVL200)



Note: The Linksys RVL200 does not support multiple tunnels. If a tunnel has already been created, you may edit its parameters, or else delete it (and then add a new tunnel).

Figure 21 Example IPSec VPN Tunnel definition in Linksys RVL200 router

Note that the customer's termination address for the VPN (the customer's VPN's global IP) is obscured in this example. However, the IP address for the "Local Security Gateway IP" should be set to the actual value. The subnet's IP address and subnet mask for the local network should be set to an internal IP.

Similarly, the "Remote Security Gateway" should be set to the Service Provider's (Wyless) VPN termination IP address (also obscured in this example). The remote network IP address and subnet should be set to the mobile device subnet, in this case given by 10.120.82.0/24.

Other sections on this page are configured using the parameters previously agreed upon, including:

Security Infrastructure Parameters Includes those in the "VPN Parameters" section of the Wyless VPN provisioning form, such as.

- The protocol used for key exchange. This example uses IKE with a pre-shared key. Other protocols are possible, if agreed upon beforehand.
- The Diffie-Hellman (DH) group was recommended (and accepted) to be 2.
- The encryption method, hashing, hashing method, and session lifetime parameters were recommended to be 3DES, MD5, and 86400. These parameters were used in both Phase 1 and Phase 2. The "Phase 2 SA Life Time" parameter has a maximum value of 28800 seconds, so this value was used instead of 86400.

Additional Parameters Other parameter guidelines on this IPSec VPN page are as follows:

- "Keep-Alive" should be checked. This specifies the creation of a static connection.
- A "Tunnel Name" should be entered, but it has no actual effect on the connection.

Final State

Note: Apart from the changes to default configuration mentioned previously, no additional changes are necessary to create the VPN connection.