



Remote Cellular TCP/IP Access to Rockwell Ethernet and Serial Devices

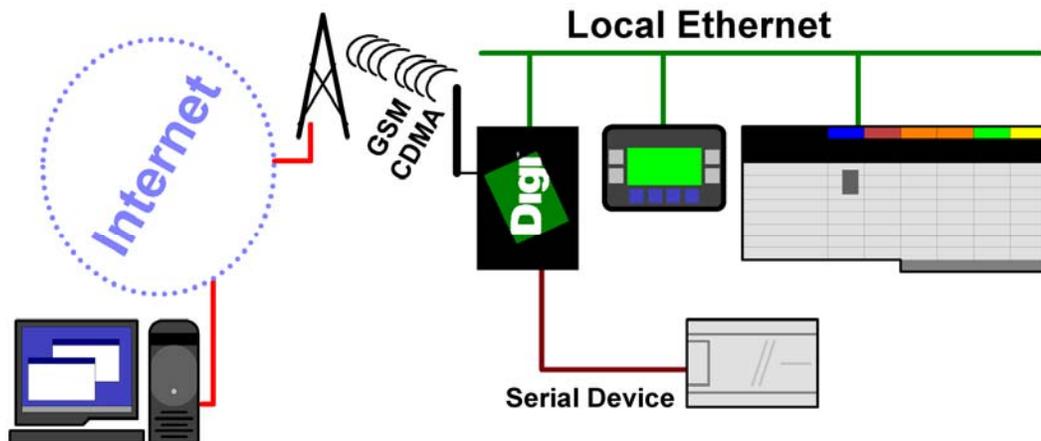
Keywords: Cellular, SLC5/05, ControlLogix, MicroLogix

Abstract: This document describes how to set up the Digi Connect™ WAN products (Digi Connect WAN, Digi Connect WAN RG, and Digi Connect WAN VPN) for remote cellular TCP/IP access to Rockwell equipment, such as the PLC5E, SLC5/05, ControlLogix, and MicroLogix. The Digi Connect WAN Family functions much like a home DSL/Cable modem, except the connection is by digital cellular signals such as GSM or CDMA. This enables wireless “Ethernet” solutions on a metro, regional, or global scale.

1 Introduction

1.1 Example Application

To illustrate the use of Digi Connect WAN products with your Rockwell equipment, consider the following example:



Key Features:

The Digi Connect WAN product used with your Rockwell equipment provides several key features:

- Provides outgoing Network-Address-Translation (NAT) and incoming TCP/UDP port forwarding. Some models act as VPN end-point.
- Maintains an always-up IP connection, either on either the public Internet or by customized private networks established through your cellular carrier.
- Being IP-based, all common Ethernet protocols can be used concurrently, including HTTP (Web browsing), ODVA Ethernet/IP, CSPv4, and Modbus/TCP.



- Existing applications, such as RSLinx, RSLogix and OPC, can be configured to access the field equipment through existing corporate LAN connections.
- Intelligent field devices can use IP-based protocols to send email, file updates, or report-by-exception notifications.



2 The Digi Cellular Family

The Digi Cellular Family includes three models to better target your needs. Here is a brief comparison of the product features:

| Feature | Digi Connect WAN VPN | Digi Connect WAN RG | Digi Connect WAN |
|--|----------------------|---------------------|------------------|
| 1) Remote TCP/IP connection to local Ethernet-enabled equipment | Yes | No | Yes |
| 2) Local Ethernet-enabled equipment can use TCP/IP protocols out to remote servers | Yes | No | Yes |
| 3) VPN end-point securely "grafts" local Ethernet onto remote network | Yes | No | No |
| 4) Remote access to local serial port by raw TCP, UDP, SSH or SSL/TLS | Yes | Yes | Yes |
| 5) Enables remote console management of routers and servers | Yes | Yes | Yes |
| 6) Interacts with standard routers for redundant (backup) paths | Yes | No | Yes |
| 7) Digi RealPort® supports legacy serial-only applications | Yes | Yes | No |
| 8) Digi configuration by remote, Ethernet, or serial connection | Yes | Yes | Yes |
| 9) Digi acts as local DHCP server | Yes | No | Yes |



Following is a detailed discussion of these features:

2.1 Remote TCP/IP connection to local Ethernet-enabled equipment

The Digi Connect WAN and Digi Connect VPN allow remote TCP/IP clients to access local Ethernet devices by TCP or UDP port forwarding. Since the Digi Connect WAN device is represented externally as a single IP address, this forwarding limits most protocols to a single local Ethernet device. However, protocols that support configurable port numbers – such as web browsers – allow forwarding to multiple local Ethernet devices.

For example, by forwarding TCP port 2222 (CSP) to a SLC5/05 and TCP/UDP port 44818 and UDP port 2222 (Ethernet/IP) to a ControlLogix, both can share the same incoming cellular connection. But two ControlLogix PLCs could not share the same connection, since TCP port 44818 can only forward to one local IP address. Web browsers routinely are assigned other port numbers such as 8000 or 8080, which are accessed as <http://192.168.1.20:8000> or <http://192.168.1.20:8080>. A VPN connection overcomes these limitations (see 2.3 VPN end-point securely “grafts” local Ethernet onto remote network below).

2.2 Local Ethernet-enabled equipment can use TCP/IP protocols targeted at remote servers

The Digi Connect WAN and Digi Connect WAN VPN support Network-Address-Translation (NAT) and thus allow any number of local Ethernet devices to act as outgoing TCP/IP clients to access remote servers.

For example, any number of local PLCs could use MSG blocks to send unsolicited or report-by-exception data back to the central site. Since TCP/IP is being used, HMI devices can send email, FTP, and even HTTP to push data to other sites.

2.3 VPN end-point securely “grafts” local Ethernet onto remote network

The Digi Connect WAN VPN can establish a Secure IPsec (VPN or Virtual Private Network) connection back to a VPN server at your corporate site. Once this is established, the entire local subnet appears to be attached and reachable from your corporate network. This overcomes the security and access limitations mentioned in section 2.1 above.

For example, the Digi Connect WAN VPN uses the cellular-assigned IP address to connect and securely authenticate with a central VPN server. The Digi Connect WAN VPN can even have a dynamic IP address. Once connected, the cellular link and Digi Connect WAN VPN disappear from the connection and the local subnet is securely accessible from the central site. For example, a company with 200 remote sites could address the remote sites as 10.75.x.y, where “x” selects 1 of 255 remote subnets and “y” selects end devices.

2.4 Remote access to local serial port by raw TCP, UDP, SSH or SSL/TLS

Digi Connect WAN, Digi Connect WAN RG, and Digi Connect WAN VPN allow remote clients to open TCP sockets which access the serial port. By



encapsulating a serial protocol into this socket, the remote clients can access the attached serial device.

For example: an OPC server can encapsulate DF1 or Modbus/RTU into a TCP socket and communicate to an existing serial PLC at site. The OPC server and PLC would need to support longer timeouts to accommodate the added latencies in a wide-area network connection.

2.5 Enables remote console management of routers and servers

The Digi Connect RG, WAN, and VPN allow remote login on serial console port for routers and servers, offering diverse out-of-band management for land lines.

For example, a Cisco router manages IP traffic over several land lines for an Ethernet subnet at a remote pumping station. If one of the land lines goes down, network maintenance people cannot access the router by network to troubleshoot. However, the cellular link through the Digi Connect WAN product allows them to log into the router and troubleshoot the situation.

2.6 Interacts with standard routers for redundant (backup) paths

Digi Connect WAN and Digi Connect WAN VPN support router protocols and can coordinate with traditional land-line routers, including those by Cisco. This allows normal IP traffic to use dedicated land-lines such as frame relay or ADSL links, but to automatically fail over to cellular service when required.

2.7 Digi RealPort[®] supports legacy serial-only applications

Digi Connect WAN RG and Digi Connect WAN VPN support the Digi RealPort[®] protocol. A serial-port driver is loaded under Windows, Linux, and most other common operating systems. This driver makes the remote port to appear as a physical serial port on the computer. This allows legacy applications that expect physical serial ports to work with your remote devices. More information on Digi RealPort[®] can be found at http://www.digi.com/pdf/fs_realport.pdf

For example: Digi RealPort[®] creates a COM2 on the computer which links to a remote Digi Connect RG or VPN. A configuration tool that only works with COM1 to COM4 can be used to configure a remote device. Of course the tool and device need to support longer timeouts to accommodate the added latencies in a wide-area network connection.

2.8 Configuration by remote, Ethernet or serial connection

Digi Connect WAN, Digi Connect WAN RG, and Digi Connect WAN VPN can be configured either remotely, by direct Ethernet, or by RS-232 connection.

2.9 Acts as local DHCP server

Digi Connect WAN and Digi Connect WAN VPN can act as a DHCP server for local Ethernet devices.



3 Performance Expectations

3.1 LAN and WAN Differences

In theory, any TCP/IP-based or UDP/IP-based protocol will work fine over any IP-based Wide Area Network. However, implementers unconsciously build in LAN timing assumptions that prevent their products from running successfully over WAN. In general, satellite and cellular networks require software to be patient. Prematurely timing out and retrying when the network is busy makes matters worse, can actively prevent lost communications from recovering, and can increase your communication costs a hundred-fold.

Here is a brief comparison of differences between “Ethernet” and “WAN”:

| | Ethernet (LAN) | Satellite / Cellular (WAN) |
|--|--|--|
| 1) Connection Delay: how long to “open a socket” or “close a socket” | Normal: less than 0.2 second. Maximum: assume 5 or 10 seconds is failure. | Normal: 2 to 5 seconds. Maximum: must wait 30 to 60 seconds before assuming failure. |
| 2) Reconnection effort: how hard to “try to reconnect” | Applications try to reconnect either fairly aggressively within seconds, or they just fail and expect user intervention. | Because retries cost money, applications must not retry any harder than the normally budgeted communications. |
| 3) Response Delay: how long to “wait for a response” | Normal: less than 0.2 second. Maximum: assume 1 or 2 seconds is failure. | Normal: 1 to 3 seconds. Maximum: must wait at least 30 seconds before assuming failure. |
| 4) Idle TCP sockets | TCP sockets can sit idle indefinitely; limited only by application protocol expectations. | Varies, but many WAN systems ungracefully interfere with idle TCP sockets; they may stop working without either end seeing a close, abort, or reset. |
| 5) UDP reliability | On modern 100M switched Ethernet, UDP/IP is actually quite reliable with packet loss rare. | Loss of UDP packets is to be expected and can be a sizable percentage of total traffic. |
| 6) Costs to Communicate | Only cost of generating network messages is the impact on other devices and communications. | Most WAN systems include costs based on maximum expected data bytes per month; every message sent potentially costs money. |

3.2 Will my application work?

Unfortunately, most product developers only test on Ethernet/LAN; it is very possible that the first users attempting to use WAN will have to locate and point out the problems for the developers.



3.2.1 Connection Delay

Connection delay is likely the largest problem you will have. Most applications use the OS defaults – on Windows, this connection delay generally is 5 seconds. Since the application may not even manage an internal setting for connection delay, users won't have any option to change this default behavior. So even if the application allows users to define a 30-second response timeout, the initial socket open will still time out too fast.

What does this mean?

- In a best-case scenario the application does not wait long enough to open a socket, making reconnection difficult at times. As long as the application waits at least 30 second before it retries, the connection it will eventually recover.
- However, the worst-case scenario occurs if the application not only times out too fast, but retries too fast. In that case, the TCP peers in effect alternate between acting as if they are connected but having to “reset” the connection due to timeouts, and assuming they need to retry the connection. This behavior could continue for as long as the network is congested, and can result in huge overage charges of hundreds or even thousands of dollars in a single month.

3.2.2 Reconnection Effort

Many applications offer users little or no control over the effort spent to reconnect after a TCP/IP connection failure. For example, a customer may configure the application for one remote poll each 5 minutes and assume they will incur less than 5MB of data charges per month. However, this application may very aggressively attempt to reconnect during network failure and literally generate more than 1GB of excess traffic in a few days. This can result in thousands of dollars of overage charges per device when the monthly bill comes.

What does this mean? Although the user “asked” the application to only talk once every 5 minutes, the application isn't really agreeing to this. Users need to confirm their applications can be configured to sharply limit attempts to reconnect. If the user budgets to only talk once every 5 minutes, ideally the application will also attempt to reconnect only once every 5 minutes and generate roughly the same amount of traffic as the normal 5 minute polls.

3.2.3 Response Delay

Many applications default to assume Ethernet/LAN responses occur in 250 milliseconds or less. Fortunately, most applications allow users to change this value. Unfortunately, some applications limit the maximum response delay to 5 or 10 seconds. A WAN-aware application should allow this setting to be at least 30 seconds, and preferably at least 60 seconds.

What does this mean? Besides the obvious performance problems when too many timeouts repeatedly puts the remote device “off-line”, a more risky problem is how the application handles unexpected responses (technically, “no-longer expected” responses). A simple example is an application that sends a



request, then timeouts twice and tries twice. How will the application react when it receives three responses at the same time? Remember, the first two requests were not *lost*; they still reached the remote device. Their responses were just delayed longer than expected.

3.2.3.1 Idle TCP Sockets

Idle TCP Sockets are related to item #5 (Cost to Communicate). The obvious solution to reducing cost is to slow down data polls. However, at some point, the idle TCP sockets become "unreliable". The sockets are not unreliable in a UDP/IP sense, but in that the application thinks it has a valid TCP socket, but it does not. The application will send a packet, wait, and see no ACK or other indication the socket is closed. So it will follow the normal TCP rules of back-off and retry. But this activity is in vain, as the only solution will be to abort (not close) and then reopen the socket.

This issue varies based on WAN technology, but a good rule of thumb at present is that you must either send data or a TCP keep-alive every 4-5 minutes to keep the TCP socket healthy.

3.2.4 UDP Reliability

UDP reliability may seem like a moot point; by definition UDP/IP is unreliable. An application using one or two UDP packets per transaction will likely handle WAN fine. The big problem arises with applications that require tens of thousands of sequential UDP packets to complete a single transaction, such as TFTP for file transfer. The longer response lags and higher probability of UDP packet loss may prevent the application from ever completing the transaction.

However actual cellular tests with UDP/IP show it to be very reliable compared to traditional analog modems. Users can expect 1 or 2 lost UDP packets per 10,000 packets sent. This compares very favorably to traditional analog modems where errors were expected every few hundred packets.

3.2.5 Cost to Communicate

Few applications are written to optimize network traffic; after all, it is usually the end devices themselves and not the "Ethernet" which is the limiting factor. But put such applications across a WAN, and you may discover that 99% of the data you are paying for is either protocol overhead or data updates without any change in value. Here are some example monthly data usages based on 200-byte transactions

- 200 bytes per second = 518M/month
- 200 bytes per 5 seconds = 86M/month
- 200 bytes per minute = 9M/month
- 200 bytes per hour = 0.14M/month (likely treated as 0.78M due to round-up)

Remember the issue above requiring TCP sockets to move data every 4-5 minutes. Ultimately, to minimize cost applications may need to be rewritten to implement Report-By-Exception or Change-of-State – preferably by UDP/IP.



3.3 IP Address Considerations

In general there are three types of “service plans” for IP address assignment that you can contract.

3.3.1 Proxy or Private (Hidden) IP address

The lowest-cost service plan will be a Proxy plan, where the Digi device is assigned a private, non-routable IP address, such as 10.x.x.x. Your service provider appears to be a huge “home network” that allows outgoing connections but prevents all incoming connections. This service plan only works if your field device initiates all communications to your central server. Since the IP address is unreachable from your central server, even attempting to ‘send’ the IP address to your server will not enable it to initiate a response.

3.3.2 Internet or Public (Exposed) IP address

In an Internet or public (exposed) IP address plan, the Digi device is assigned a dynamic public IP address, such as 166.x.x.x, plus the service provider usually maintains a DDNS server allowing you to locate the Digi device by a DNS lookup. Your field device can initiate communications to your central server. Your central server can use DNS lookup to initiate communications to your field device. Since the IP address is fully exposed as public, others are free to probe and attempt to connect to your field device.

3.3.3 Custom plan with fixed IP address and other options

In a custom plan, you arrange IP addresses with your service provider as required. Most large users will arrange a 100% private and hidden network based on fixed IP addresses. However, custom plans generally cost extra, or are reserved for larger customers with hundreds of cellular devices.

3.4 What about the advertised “Unlimited Data Plans?”

Unfortunately, the “unlimited data plans” are not for you. Cellular carriers split data plans into two types of service:

- The largest group of data users consists of a mobile phone, PDA, or notebook computer in the hands of a human user. The mobile device is connecting out to the Internet; in fact it is likely impossible for a remote server to ever connect to the mobile device. Carriers know that the human user driving these devices normally use no data at all, and only use large amounts of data for short bursts of time, so the notion of “unlimited data” is tolerated.
- In contrast, the other group of data users can be referred to as “machine-to-machine” or M2M. Such a telemetry system can easily consume its full bandwidth 100% of the time forever. In these situations, a central server or “the Internet” is connecting out to the remote mobile device. Cellular carriers require M2M users to sign up for “Telemetry Data Plans” – none of which offer unlimited data once you read the fine print.



3.5 Costs of continuous versus occasional access

For continuous access, the number and frequency of polls determines if your monthly bill will be \$20 or \$2000. You need to run some carefully controlled pilot tests to confirm whether your existing software tools are compatible with a high-latency system like cellular. Some software tools work fine when the network is up, but have recovery behavior that multiplies the data moved by 100 or more times. Therefore, make sure you test the data moved during system failures. Remember, it is not the data that reaches your cellular device for which you are charged. Instead, you are charged for the data that is * **SENT** * to your cellular device regardless of whether your device is even powered up. Therefore an application that tries too hard to stay connected or reconnect is not suitable for use with a cellular network.

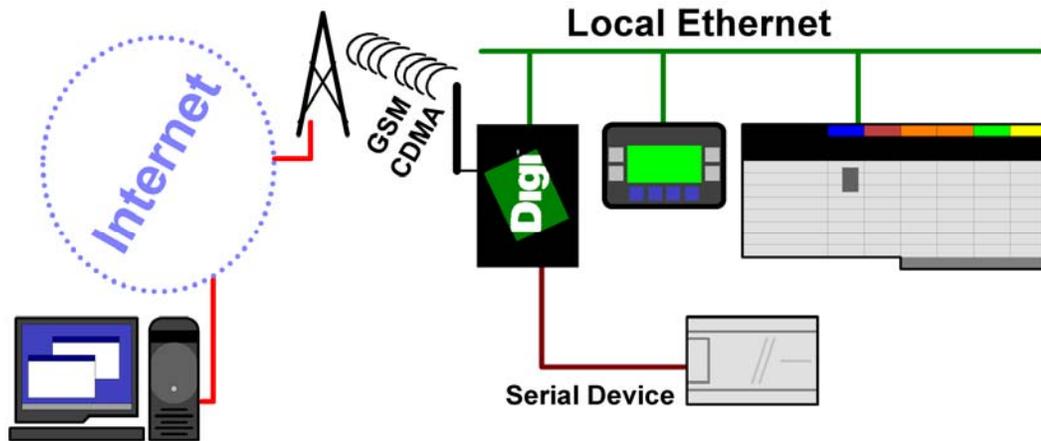
Your task is simpler if you plan on occasional access only. You can view the costs much like long-distance telephone costs. Real-world PLC tests show that connecting with programming tools causes from 5k to 25k of data to move per minute. For your average cell plans – assuming you have already used up your “included kilobytes” – this works out to be from \$1 to \$12 per hour to connect. While you would not want to pay \$12 per hour to connect for 72 hours (that is, \$864), troubleshooting a PLC for an hour or two at \$12 per hour is cheaper than either sending an engineer to site or dialing up to an analog modem with normal business-to-business long distance charges.



4 Cellular-Enabling Ethernet Devices

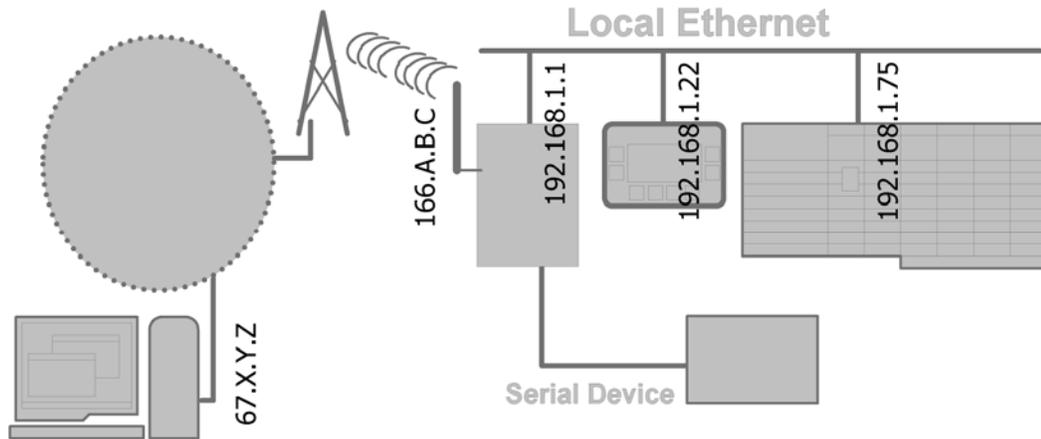
4.1 Overview

The Digi Connect WAN and Digi Connect WAN VPN act much like your home DSL/Cable router. It is assigned an IP address by your service provider (your “cellular ISP”). Outgoing TCP/IP connections are handled with Network Address Translation (NAT), just as your home DSL/Cable router does. This allows any number of local Ethernet devices to connect out into the Public Internet. However, to the Public Internet, the Digi Connect WAN or Digi Connect WAN VPN appears as just a single IP address. Therefore, incoming connections must be manually forwarded based on TCP port number to one and only one of the local Ethernet devices. That restriction means it is not possible to have more than one Modbus/TCP device expecting connections on TCP port 502 or Ethernet/IP device expecting connections on TCP port 44818.



4.2 IP Address Design

Here is an example of IP address assignment in a sample system, followed by a discussion of each set of addresses:



4.2.1 Local Ethernet Subnet (192.168.1.X)

In this example, all devices on the local Ethernet subnet are assigned an IP address in the range 192.168.1.1 to 192.168.1.254 with a subnet mask of 255.255.255.0. This range is defined for “private” use, meaning you do not need to ask permission or pay anyone money to use this range.

The Ethernet port of the Digi Connect WAN/Digi Connect WAN VPN is assigned the IP of 192.168.1.1, and acts as the router/gateway for the subnet. Set your other devices to any **IP in the range 192.168.1.2 to 192.168.1.254** and set their **router/gateway IP to 192.168.1.1**. Unless you are an expert at manual IP route table configuration, you cannot have any other routers on the local subnet.

Model Note: A Digi Connect WAN or Digi Connect WAN VPN (but not a Digi Connect WAN RG) can act as a DHCP server for the local subnet. While you likely want to use fixed IP addresses for your field devices, your mobile field technicians will enjoy having this server enabled to allow painless connection of a portable computer when on-site.

4.2.2 Public/WAN IP Addresses

The cellular port of the Digi Connect WAN/ Digi Connect WAN VPN is assigned an IP address by your service provider, such as 166.213.2.000 or 67.48.210.000 – which are both public IP addresses in this example.

An application on the host computer (IP 67.X.Y.Z) can open a Modbus/TCP or Ethernet/IP connection to the Digi Connect WAN device at IP 166.A.B.C. The Digi Connect WAN device must be configured to forward each desired TCP or UDP protocol to one (and only one) of the local Ethernet devices.



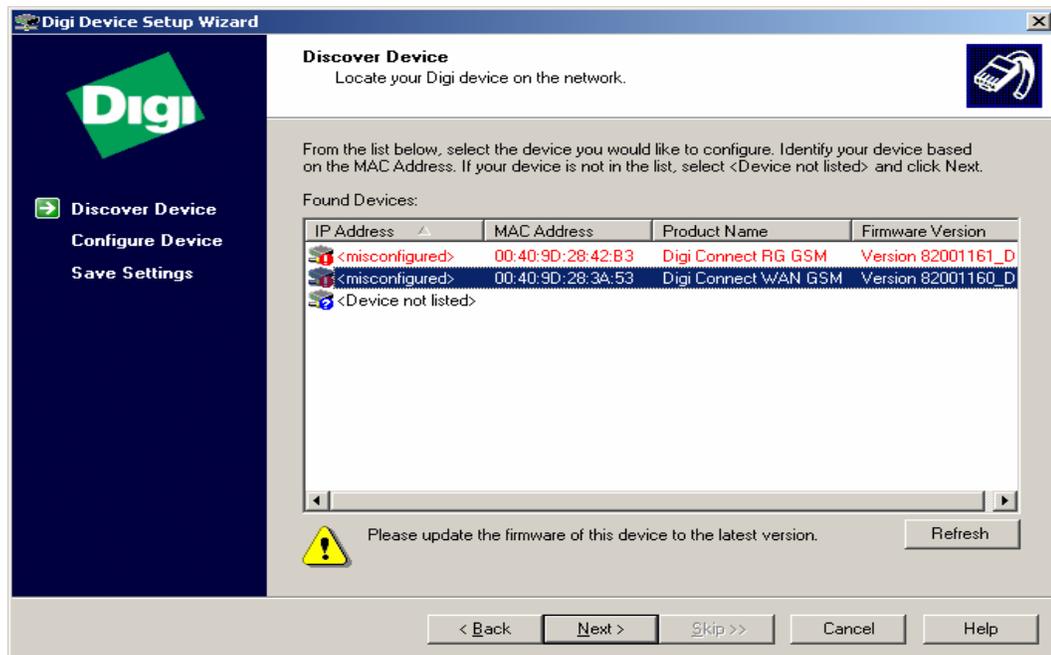
4.3 Configuring the Digi Connect WAN Device

To configure your Digi Connect WAN, Digi Connect WAN RG, or Digi Connect WAN VPN, attach both your Digi device and computer to the same Ethernet hub or switch.

4.3.1 Device Discovery and IP settings

Install the Digi Device Discovery tool that is included on the CD with your Digi device on your computer.

The Digi Device Discovery tool uses IP multicast to locate any Digi products connected to your local subnet. There are several factors that may block or affect the device-discovery operation, for example, some “Personal Firewall” products block this discovery, and some combinations of Ethernet hardware under Windows and “cross-cables” do not allow proper device discovery. If you cannot see your Digi device within the device-discovery results after a few minutes and after pressing **Refresh**, try using an external switch (not a cross-cable) and disable any personal firewall to allow full network access.



The “<misconfigured>” warning in the device discovery results above is caused by the Digi device having an existing IP address assigned on a different subnet. For example, your PC may have the IP address 192.168.1.201 and the Digi Connect WAN/an IP address of 192.168.20.1. This does not prevent the tool from changing the Digi device’s IP address information.

The **Name** field shown is the standard hostname, and can be set through the Web user interface under Network Configuration – Advanced Network Settings.

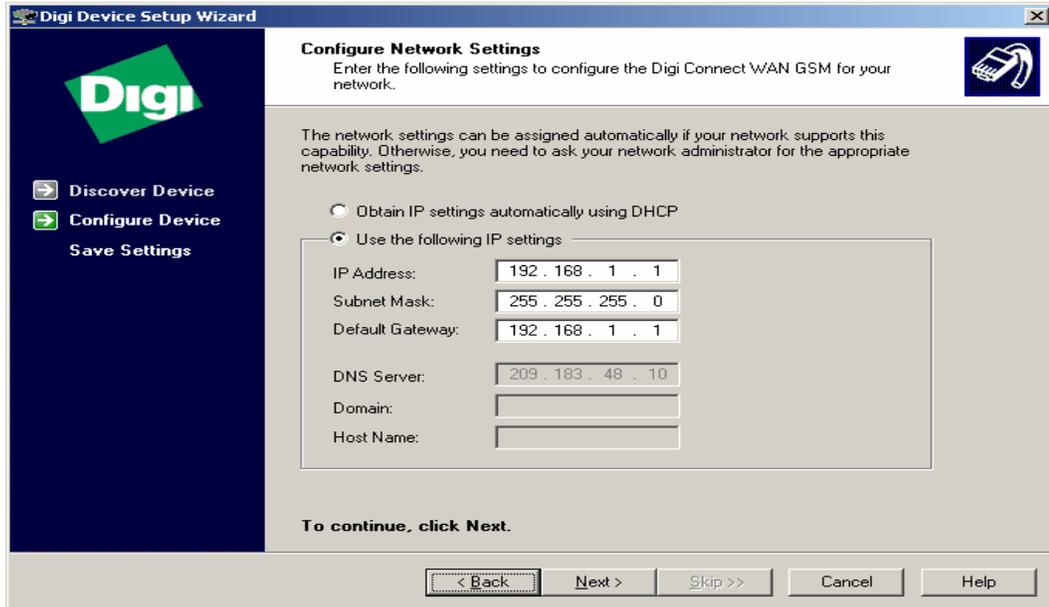
Remember that, at this point, we are just assigning the IP address used by the *Ethernet port* of the Digi device. The IP address used by the *cellular port* will be assigned remotely by your cellular service provider. Even if you have arranged



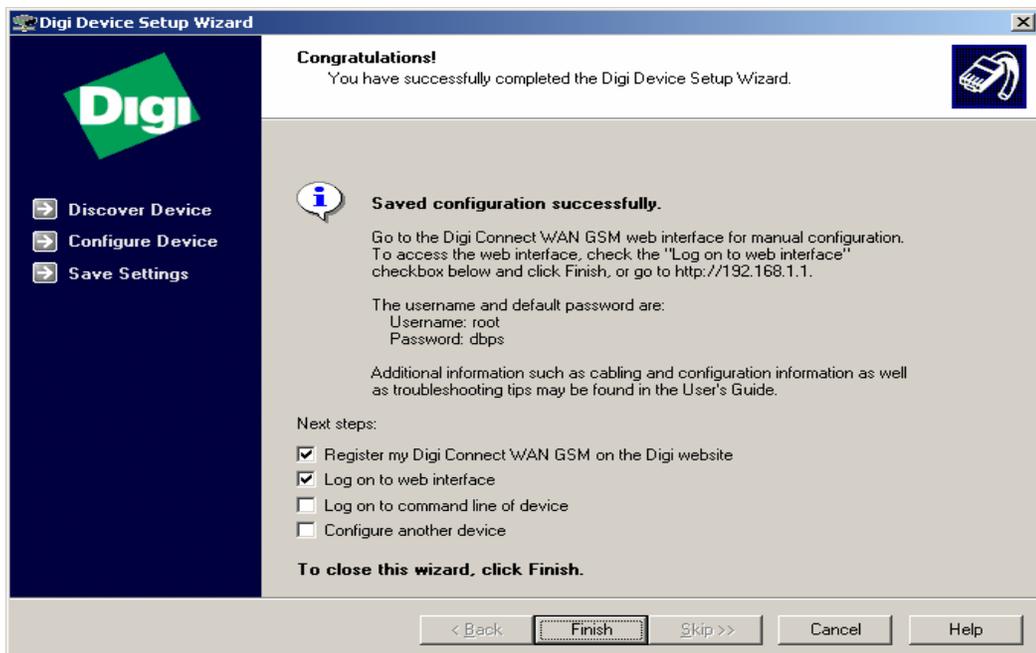
for a fixed IP address to be used, the ISP will “dynamically” reassign the same IP address every time to your cellular connection.

Select your device to configure – the Ethernet MAC address is shown by each entry – and click **Next**. The Digi Device Setup Wizard is launched. On the Configure Network Settings screen, enter the desired information, such as IP address 192.168.1.1

You can skip the Scenario Settings wizard screen, and continue to click **Next** until the wizard screen titled **Saving Settings** is displayed.



After a minute or two, you should see the **Congratulations** screen below.





4.3.2 Web Interface and Service Plan Settings

Next, open the Web user interface for your newly installed Digi Connect WAN/WAN RG/WAN VPN. You can either open the Web user interface from the last screen of the Digi Device Setup Wizard, as shown above, or launch your desired Web browser, specifying the address of the Digi device. The home page is shown below.

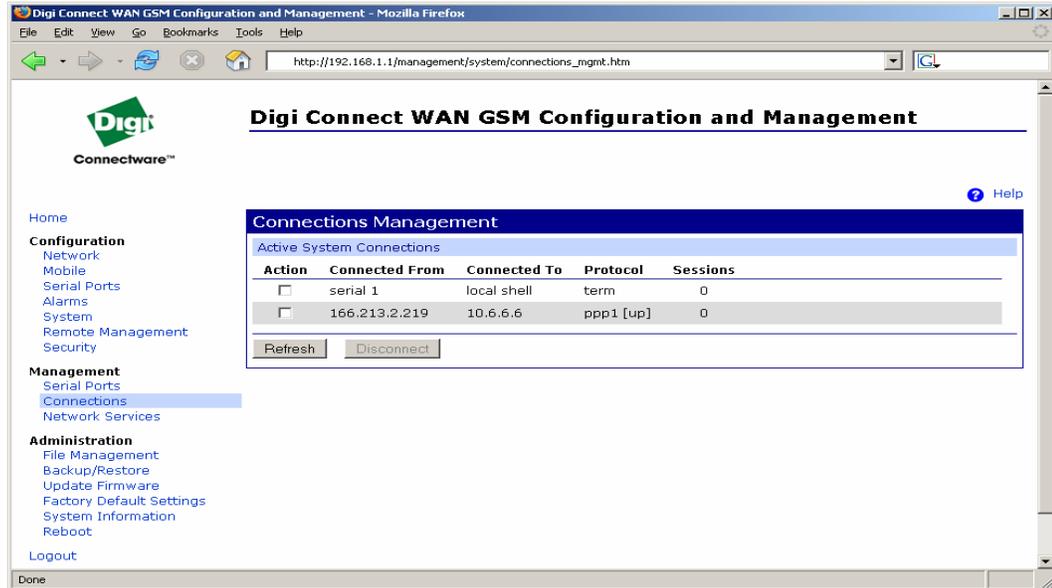
The screenshot shows the 'Home' page of the Digi Connect WAN GSM Configuration and Management web interface. The page features a navigation menu on the left with categories: Configuration (Network, Mobile, Serial Ports, Alarms, System, Remote Management, Security), Management (Serial Ports, Connections, Network Services), and Administration (File Management, Backup/Restore, Update Firmware, Factory Default Settings, System Information, Reboot). The main content area includes a 'Getting Started' section, a 'Tutorial' section with the text 'Not sure what to do next? This Tutorial can help.', and a 'System Summary' section. The System Summary displays the following information: Model: Digi Connect WAN GSM, MAC Address: 00:40:9D:28:3A:53, IP Address: 192.168.1.1, Mobile Address: 166.213.2.219, Description: None, Contact: None, Location: None, and Device ID: 00000000-00000000-00409DFF-FF283A53. A 'Logout' link is located at the bottom left of the navigation menu.

At present, your Digi Connect WAN/WAN RG/WAN VPN is not likely connected to the Internet. Under the **Configuration** menu, click **Mobile**. In the **Mobile Service Provider Settings**, enter the *information provided by your service provider* – the information shown below is an example. Pressing **Apply** initiates your Internet connection. Some carriers also require you to access a web site or telephone directly to activate your assigned data plan.

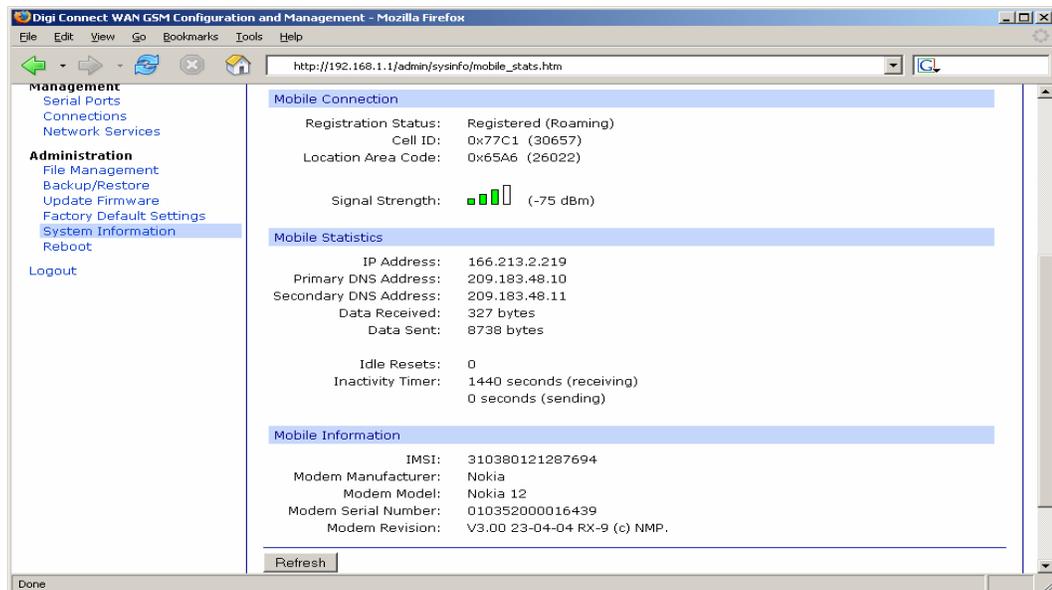
The screenshot shows the 'Mobile Configuration' page of the Digi Connect WAN GSM Configuration and Management web interface. The page features a navigation menu on the left with categories: Configuration (Network, Mobile, Serial Ports, Alarms, System, Remote Management, Security), Management (Serial Ports, Connections, Network Services), and Administration (File Management, Backup/Restore, Update Firmware, Factory Default Settings, System Information, Reboot). The main content area includes a 'Mobile Settings' section with the text 'Select the service provider, service plan, and connection settings used in connecting to the mobile network. These settings are provided by and can be retrieved from the service provider.' The 'Mobile Service Provider Settings' section includes the following fields: Service Provider: Cingular Wireless (Blue Network) (dropdown), Service Plan: Custom APN (dropdown), and Custom Plan Name: www.trial.acfes.org (text input). The 'Mobile Connection Settings' section includes a checked checkbox for 'Re-establish connection when no data is received for a period of time.' and an 'Inactivity timeout: 1440 secs' (text input). An 'Apply' button is located at the bottom of the page. A 'Logout' link is located at the bottom left of the navigation menu.



To see your IP status, , under **Management**, click **Connections**, and look for the PPP status. **[up]** means you are connected and ready to go. If you see the status cycling between **[init]** and **[connecting]**, this usually means that even though you may have a good cellular signal, the roaming partner to which you are connected to does not support the data service required for IP traffic.



Another useful status display is **Administration > System Information > Mobile**. The Mobile page shows your cellular signal, status of the “cellular link”, and the appropriate IP details if PPP has successfully connected. On this page, you will see the IP address assigned to your Digi device, as well as the DNS address or addresses for your field devices to use.





4.3.3 Your devices can connect out to the Internet

As configured, your local field devices can initiate outgoing connections to the Internet or central servers you maintain. They use the Digi device's IP address as the router to forward the connection; the Digi device uses Network-Address-Translation (NAT) to access the remote resource. For example, if a PLC connected to a server at IP address 67.43.210.56, the server would see it as a connection from the Digi device's IP address (for example 166.213.2.219) and *not* the IP address of your field device.

So, at this point you could use RSLogix MSG blocks in one, two, or more PLC to write data back to a central server or PLC with a public IP address. No one on the Internet would be able to connect to or bother any of your PLC.

4.3.4 Using the "ping" Command to Test Access

Just like all IP devices, you can use the "ping" command to test access. However, many "ping" utilities assume a short 1-second or 2-second timeout. So use the "-w" option to inform the "ping" command to wait longer for a response; below, "-w 10000" is used to set a 10-second timeout. Notice how the first response is considerably slower than subsequent responses.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The command prompt shows the following text:

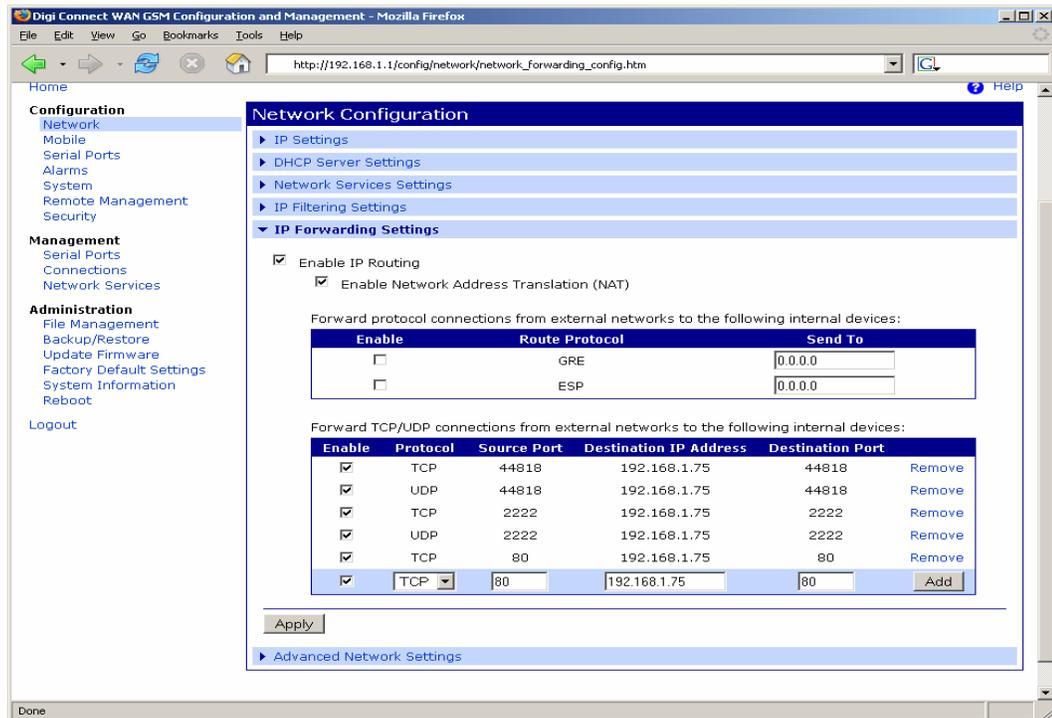
```
C:\Documents and Settings\LynnL>ping -w 10000 166.213.2.220
Pinging 166.213.2.220 with 32 bytes of data:
Reply from 166.213.2.220: bytes=32 time=2255ms TTL=45
Reply from 166.213.2.220: bytes=32 time=799ms TTL=45
Reply from 166.213.2.220: bytes=32 time=899ms TTL=45
Reply from 166.213.2.220: bytes=32 time=1038ms TTL=45
Ping statistics for 166.213.2.220:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 799ms, Maximum = 2255ms, Average = 1247ms
C:\Documents and Settings\LynnL>
```



4.3.5 Enabling Incoming Access

While outgoing connections to the Internet work with no direct configuration, to enable incoming connections from the Internet requires explicate configuration.

Select **Configuration > Network > IP Forwarding Settings**. This example assumes you have a Rockwell PLC at IP address 192.168.1.75. ODVA Ethernet/IP uses TCP port 44818 and UDP ports 44818 and 2222. The older CSPv4 protocol uses TCP port 2222. Any web server within the PLC uses TCP port 80. When all entries are added, remember to click **Apply** or you will lose your new settings.



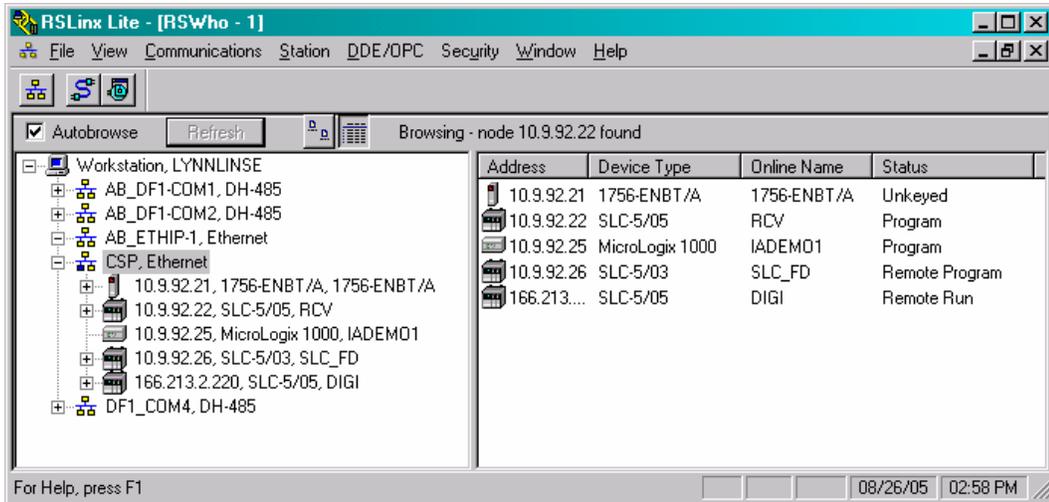
This completes the configuration steps for your Digi Connect WAN/WAN RG/WAN VPN. Now, any Rockwell protocols received by the Digi device will be forwarded to the local PLC.

Caution: As the Rockwell protocols do not include any security; your PLC is fully exposed on the Internet.

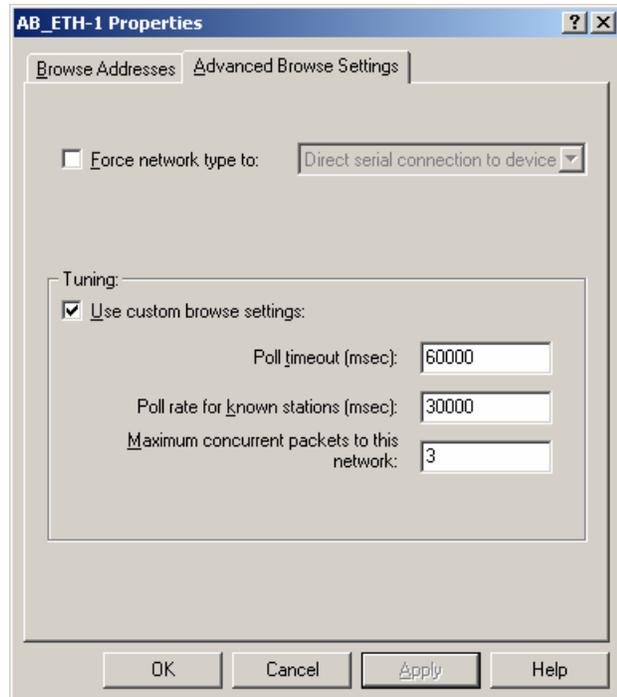


4.3.6 RSLinx 2.4x access to the remote PLC

Below is a screen shot of RSLinx accessing a SLC5/05 via a Digi Connect WAN. You must add the IP address manually to the **Station table** under the **Ethernet Device** driver. The communications to the PLC will be using the older CSPv4 protocol since RSLinx tries that protocol on TCP port 2222 first. You cannot use the Ethernet/IP driver as that relies upon UDP broadcasts to auto-detect Ethernet/IP nodes; nor can you send subnet broadcasts via cellular networks.



You must slow down the RSLinx polling behavior. To do so, select your driver, right-click, and select Properties. RSLinx uses a default of only 3 seconds (3000 msec) as the poll timeout. Increase this to 60 seconds (60,000 msec). Also, slow down the poll rate from 2 second to only once each 30 seconds to reduce excess data load.

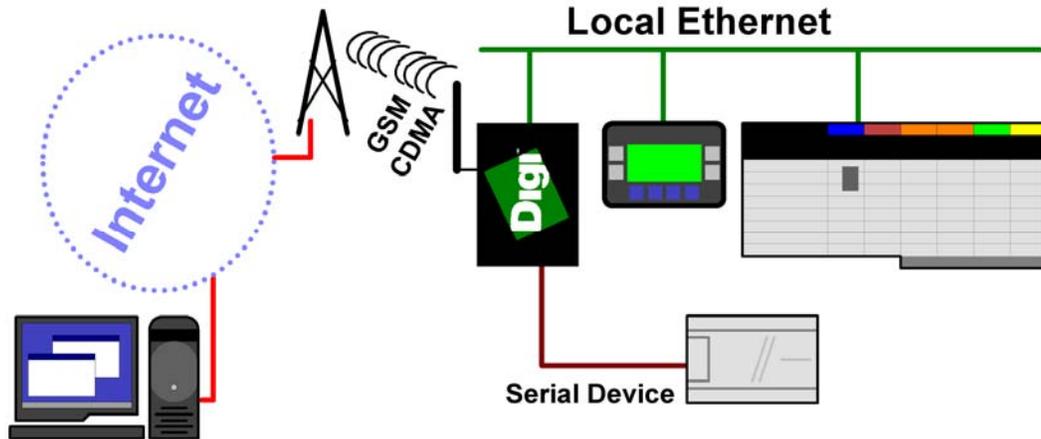




5 Cellular-Enabling Serial Devices

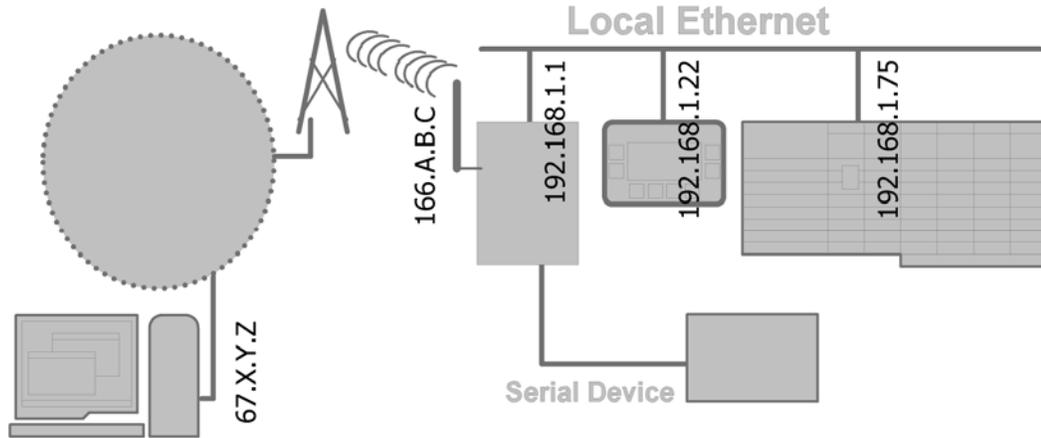
5.1 Overview

The Digi Connect WAN RG and Digi Connect WAN VPN can cellular network-enable a serial device. The Digi device is assigned an IP address by your service provider (your “cellular ISP”). In addition, the Digi Connect WAN VPN can cellular network-enable Ethernet devices on the local Ethernet – see section 3 above for details.



5.2 IP Address Design

Here is an example of IP address assignment in a sample system:



5.2.1 Local Ethernet Subnet (192.168.1.X)

All devices on the local subnet are assigned an IP address in the range 192.168.1.1 to 192.168.3.254 with a subnet mask of 255.255.255.0. This range is defined for “private” use, meaning you do not need to ask permission or pay anyone money to use this range.

The Ethernet port of the Digi Connect RG or VPN is assigned the IP address of 192.168.1.1 – only the Digi Connect VPN acts as the router/gateway for the subnet. See section 3.2.1 above for routing information.

5.2.2 Public/WAN IP Addresses

The cellular port of the Digi Connect RG or VPN is assigned an IP address by your service provider, such as 166.213.2.000 or 67.48.210.000 – both public IP addresses in this example.

5.3 Configuring the Digi Connect WAN RG/WAN VPN

Attach both your Digi Connect WAN RG/WAN VPN device and computer to the same Ethernet hub or switch.

5.3.1 Device Discovery and IP settings

Follow the procedure to set the IP address assigned to the Ethernet port of the Digi Connect RG or VPN, outlined in section 3.3.1 above. This enables you to use a Web browser to fully configure the Digi device.

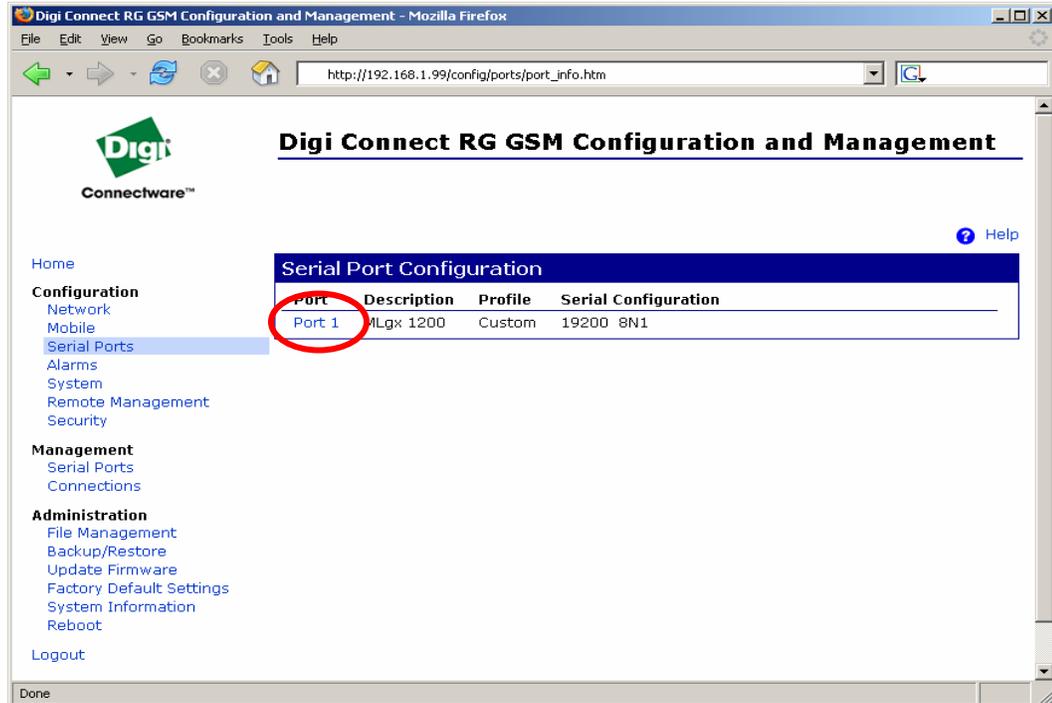
5.3.2 Web Interface and Service Plan Settings

Follow the procedure outlined in section 3.3.2 above to configure your Service Plan settings for the Digi Connect WAN RG or WAN VPN.

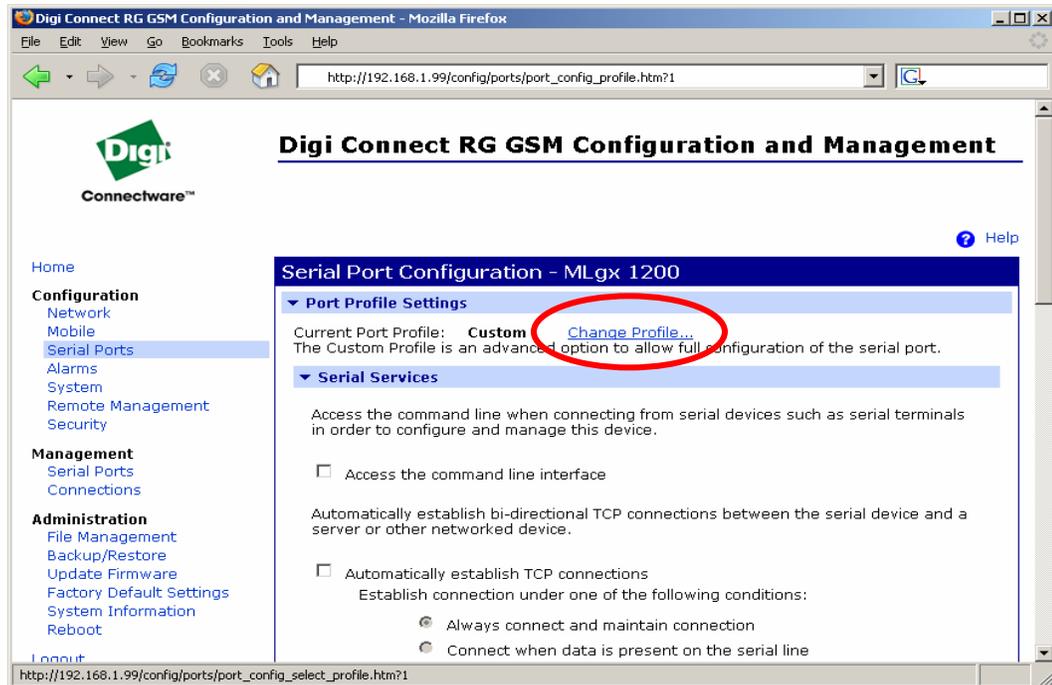


5.3.3 Configure the Serial Port

In the Web user interface for the Digi Connect WAN RG/WAN VPN, click **Configuration > Serial Ports** to see the following display. Click **Port 1** to open the Port Profile Settings page for the serial port.



Click the **Change Profile** link.

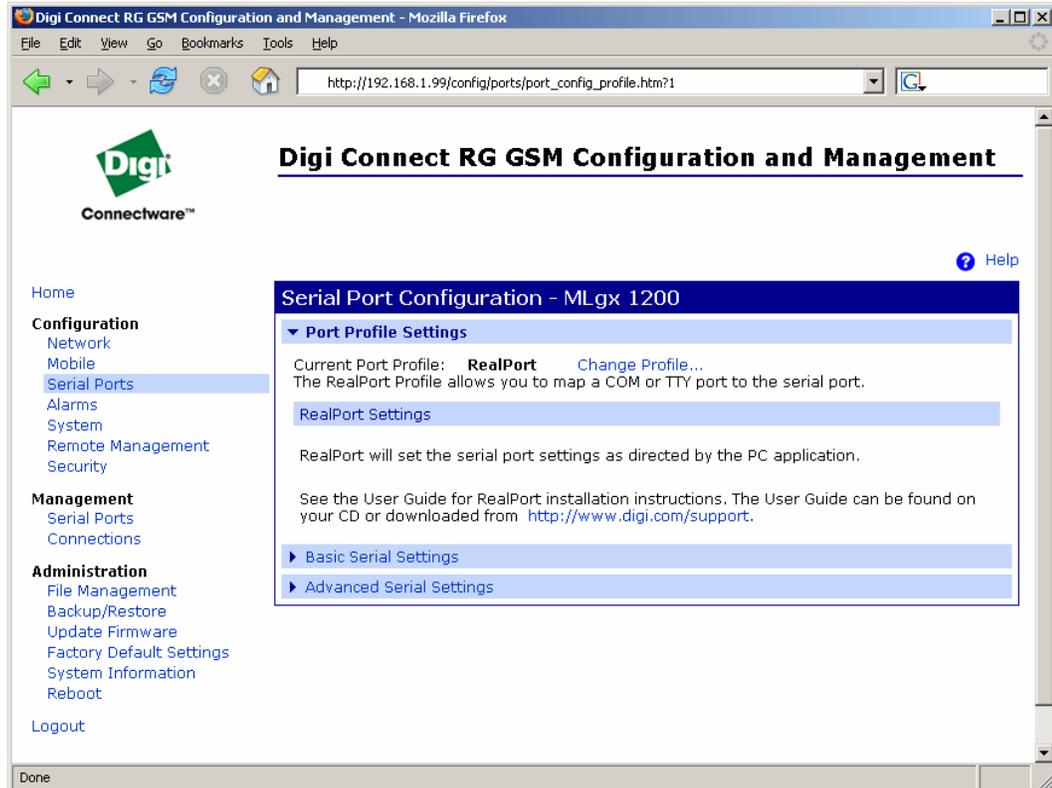




5.3.4 Configure the Serial Port – RealPort Port Profile

Select **RealPort** if you desire the serial port for the Digi Connect WAN RG or Digi Connect WAN VPN to appear to a remote computer as physical serial port. If you do select RealPort, you also need to install the appropriate Digi RealPort driver for your computer's operating system (Windows, Linux, AIX, etc.). There is nothing else you need to configure – settings such as baud rate are automatically forwarded directly from your remote application.

To use RSLinx, you'll need to select the RealPort Port Profile.

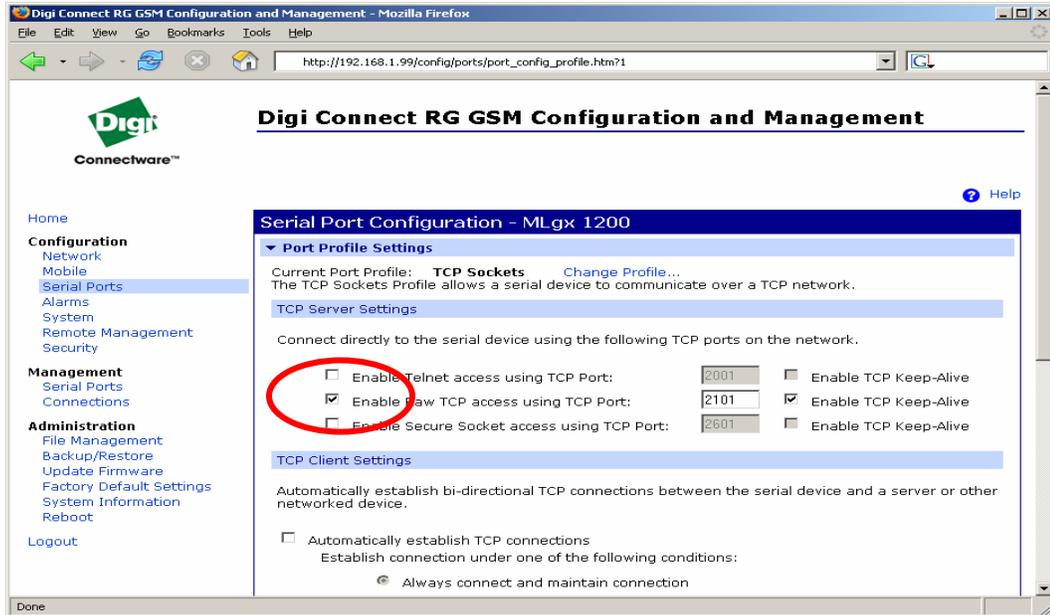




5.3.5 Configure the Serial Port – TCP Sockets Port Profile

The TCP Sockets port profile allows your remote computer to open a TCP socket to carry serial data. For example, your application can read and write DF1 messages directly into a TCP socket. Generally, you'll use only the **raw TCP port 2101** – you can change this number to any available TCP port. A growing number of OPC servers support this and call it "TCP Encapsulation".

RSLinx does not support the TCP Sockets Port Profile – use RealPort instead.

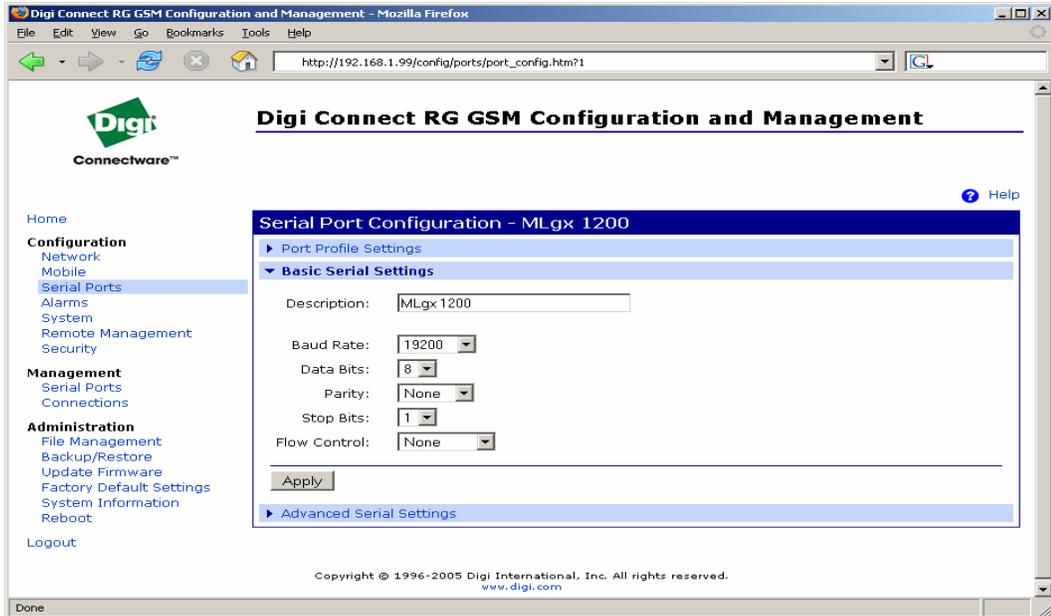


There are many options you can use, including automatically connecting out to remote TCP servers. However, explaining all options is beyond the scope of this basic application note. Select the online help link in the upper right of every page for more information.

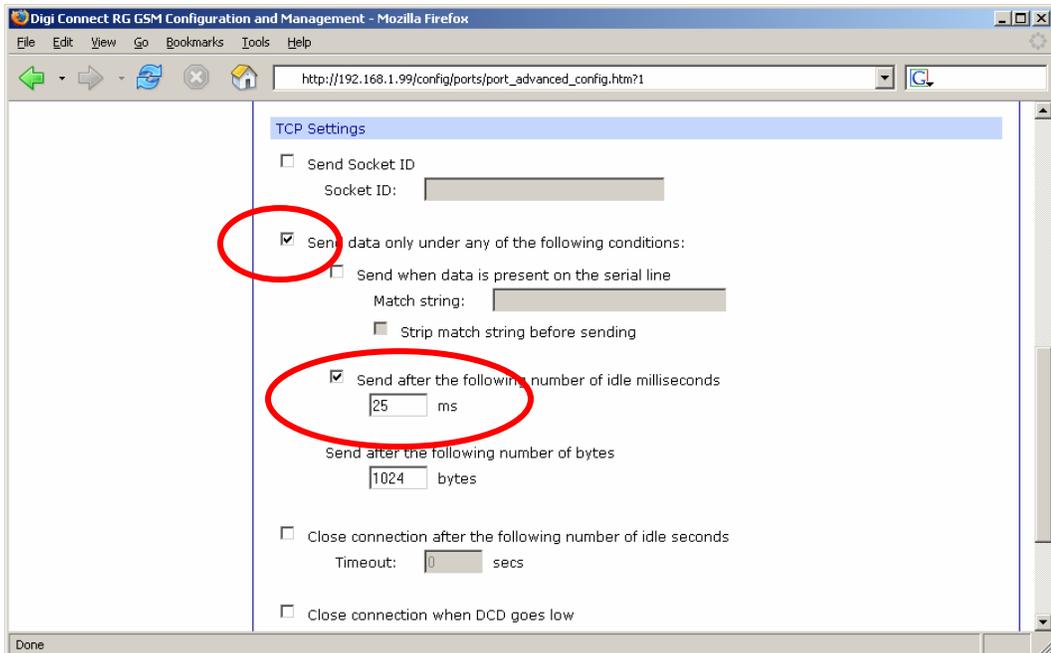
Telnet Access (default TCP port 2001) requires your application to handle Telnet commands and handle the duplication of 0xFF bytes. **Secure Socket** (default TCP port 2601) enables your application to use SSLv3/TLSv1 to open an encrypted channel to the Digi Connect WAN RG or Digi Connect WAN VPN.



Click **Basic Serial Settings**. Set the appropriate values for your Digi device; most AB PLC use **19200,8,N,1** and **Flow Control** must be set to **None**. In the **Description** field, you can enter a useful description of the Digi device.



Click **Advanced Serial Settings** and scroll down to the **TCP Settings** section shown. Enable **Send data only under any of the following conditions**. Also enable **Send after the following number of idle milliseconds** and enter the **value 25**. This prevents the Digi device from breaking DF1 responses into multiple TCP packets and trades off a small amount of speed for fewer data packets and therefore fewer monthly charges.



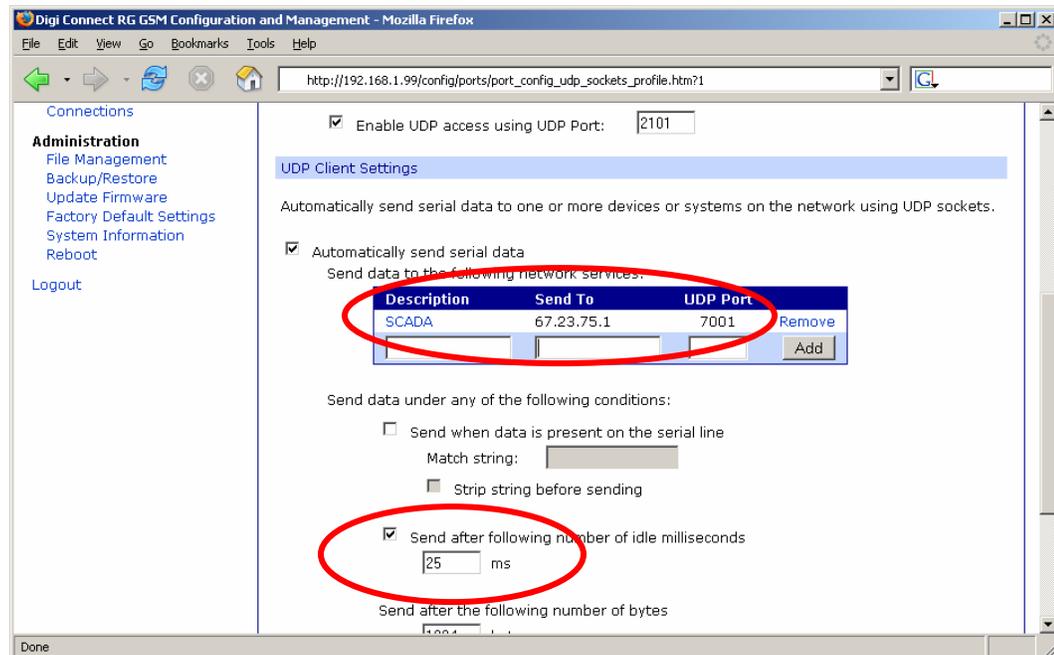


5.3.6 Configure the Serial Port – UDP Sockets Port Profile

The UDP Sockets port profile allows your remote computer to send UDP packets to carry serial data. It also informs the Digi Connect WAN RG or Digi Connect WAN VPN to which remote IP address any responses should be sent.

Enable **Automatic send serial data** and add the IP address of your central server, as shown below. More than one server can be defined, which allows for redundant data collection. Also enable **Send after the following number of idle milliseconds** and enter the **value 25**.

RSLink does not support the UDP Sockets port profile– use RealPort instead.





5.4 Install RealPort for the first time

If you have installed a previous version of RealPort, go to the Windows Device Manager and uninstall it. You should use the latest version downloadable from the Digi support web site.

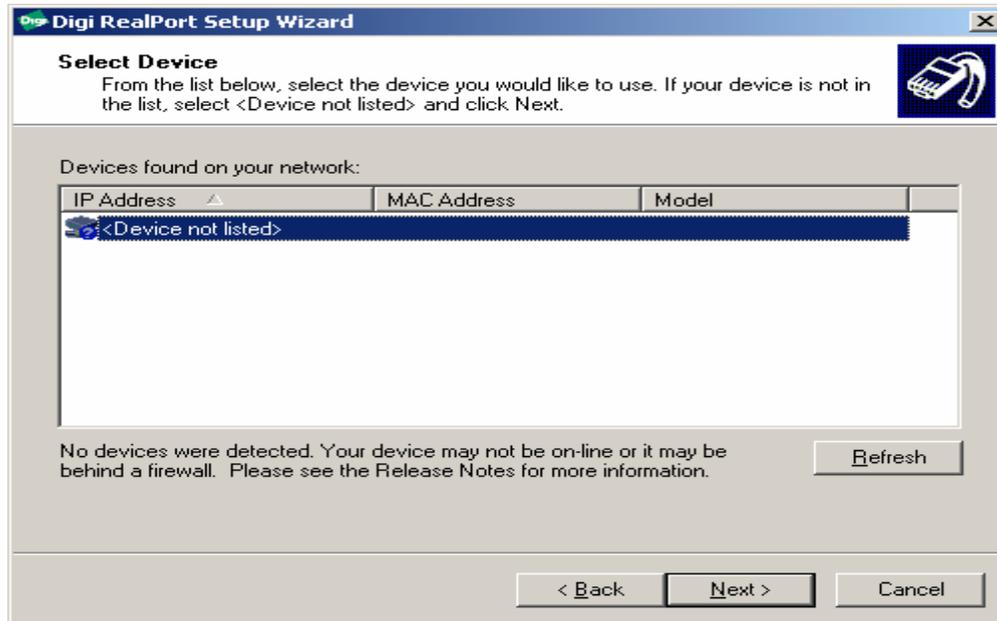
When you run Setup.exe for the first time, the Welcome screen for the Digi RealPort Setup Wizard is displayed. Click **Next**.



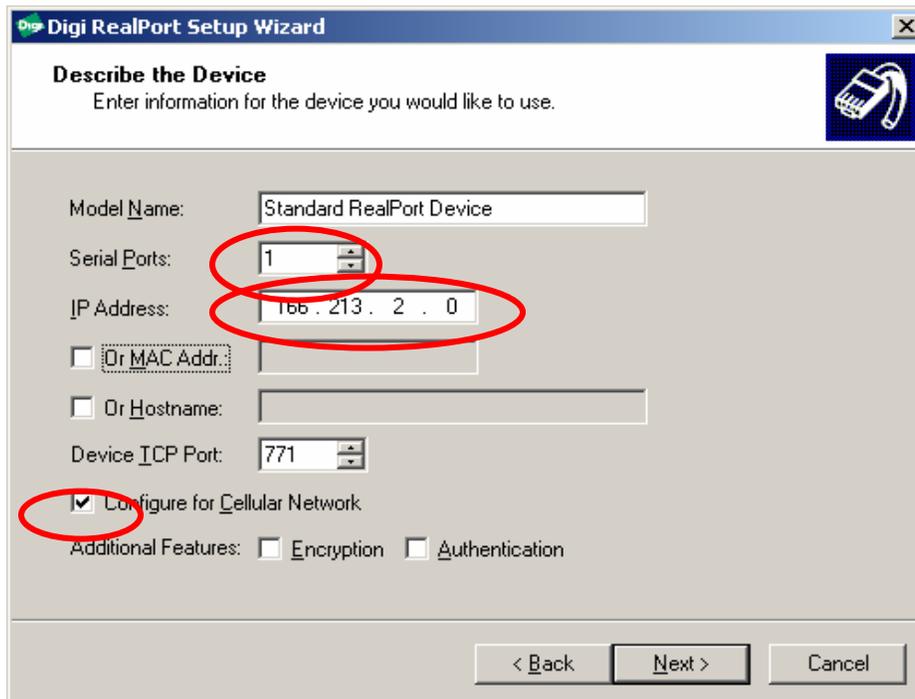


By default, RealPort probes your local subnet and finds attached Digi devices. Since the Digi Connect WAN RG or Digi Connect WAN VPN is remote, it will not be detected.

Select **<Device not listed>** and click **Next**.

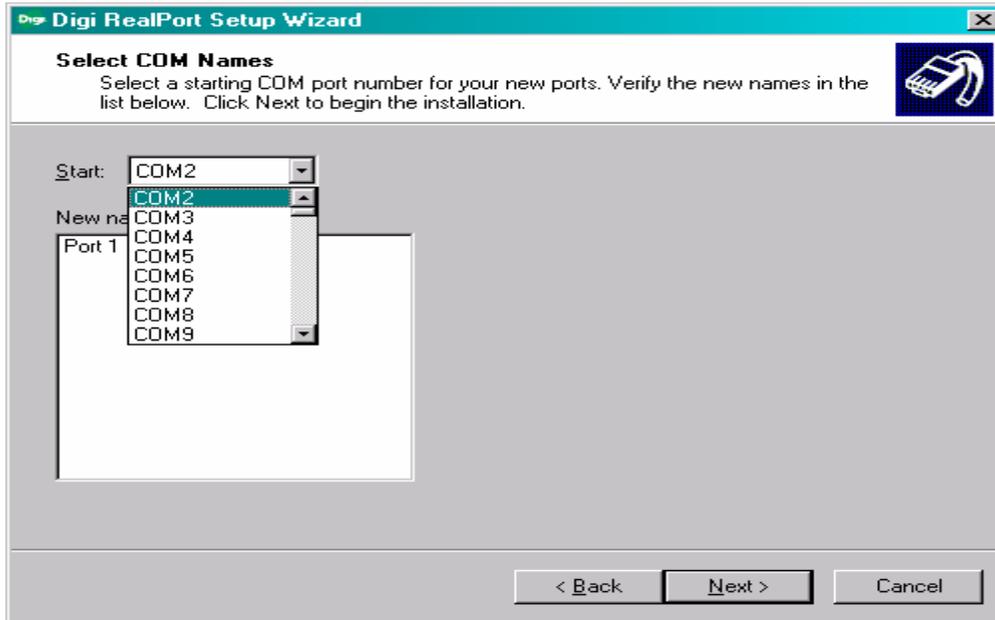


Set the **Serial Ports** to one (1) and enter the **IP Address** assigned to the Digi device. Currently, a DNS name *cannot* be used. Leave the **TCP Port** set at 771. Select to **Configure for Cellular the Networks**.





Associate this RealPort connection to any available COM port name, such as COM2 or COM31. The rest of this document assumes that you select COM2. You will only see available names reported by Windows. RealPort *cannot* “replace” an existing COM port; so, for example, COM1 will only be shown if you remove or disable the computer’s built-in serial port. Newer versions of RSLinx support up to 32 serial ports. Click **Next** to continue.



The RealPort drivers are now installed. Since RealPort will be connecting via the Public Internet to the Digi device, the actual installation may take several minutes. When installation completes, the following wizard screen is displayed.



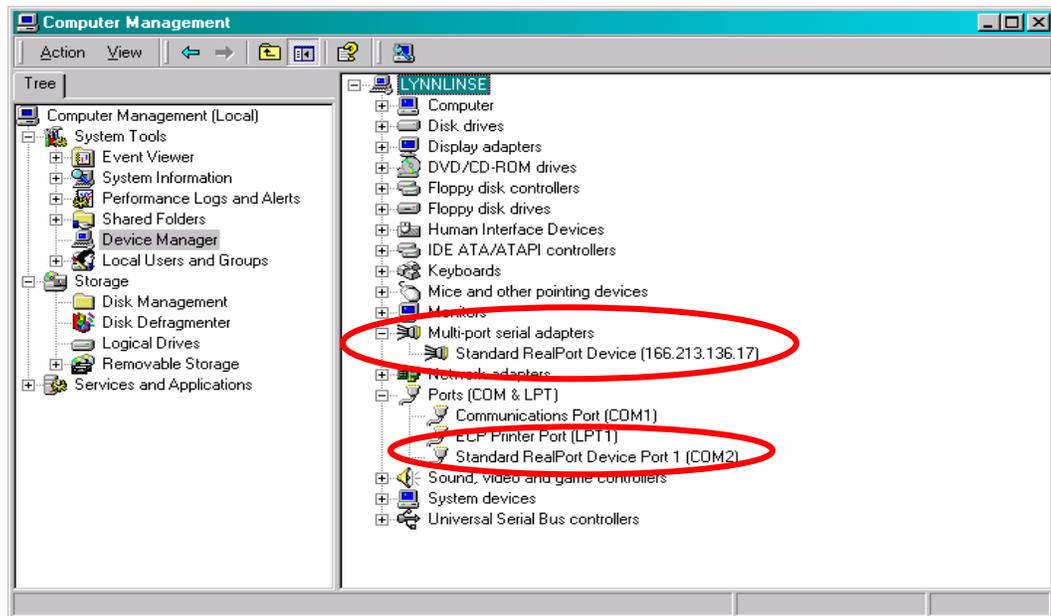


After the wizard completes, you need to configure RealPort to tolerate the wide-area network conditions of a cellular data link. Without these special settings, RSLinx can likely detect the MicroLogix 1200, but it will frequently go offline.

5.5 Configuring RealPort for Wide-Area Network conditions

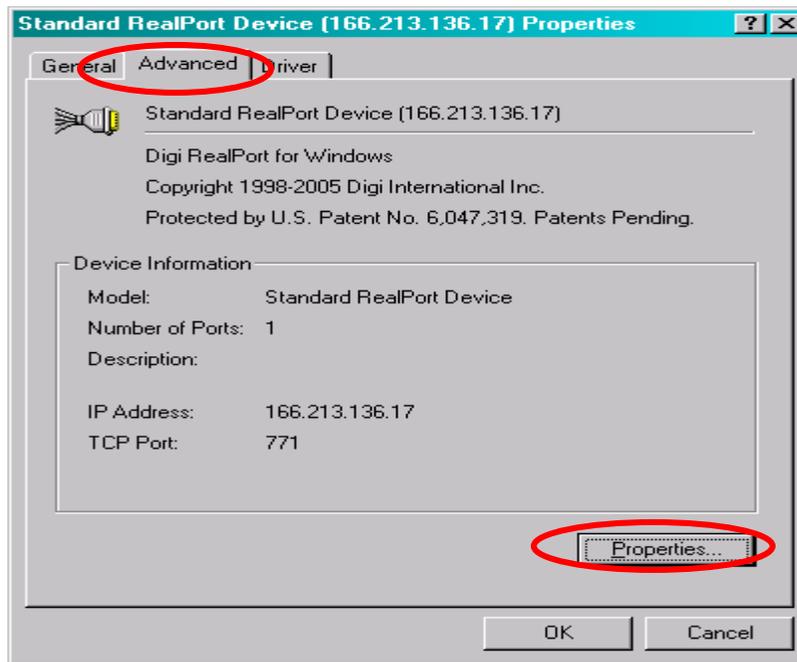
Run the Windows **Device Manager** by right-clicking the **My Computer** icon on your desktop and selecting **Manage**. In the Device Manager display, you will notice two new pieces of "hardware:"

- Each device RealPort connects has an entry under **Multi-port serial adapters**; you adjust RealPort settings here.
- In addition, each RealPort "COM port" has an entry under **Ports (COM & LPT)**. RSLinx treats the RealPort (COM2 in this case) as any other RS-232 port.

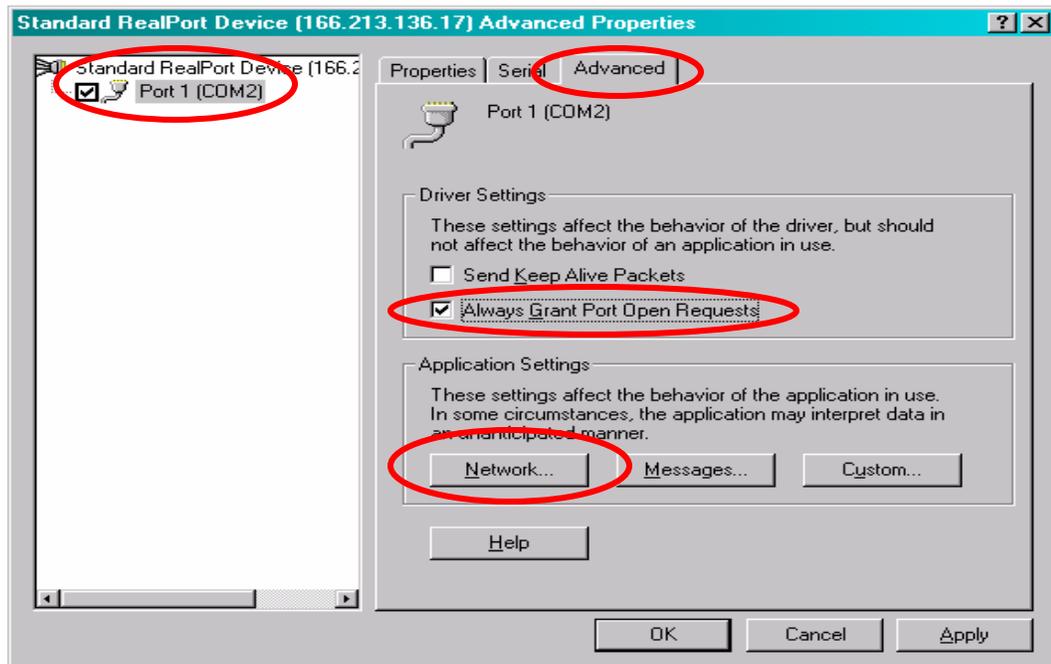




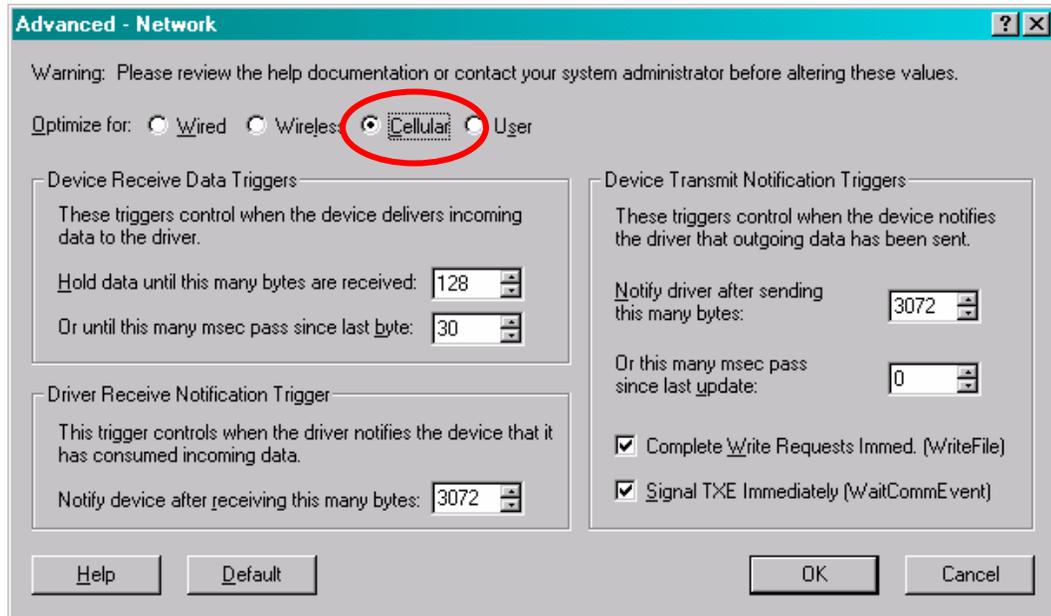
Right-click **Standard RealPort Device (166.213.136.17)** and select **Properties** in the drop-down menu. On the **Advanced** tab, click **Properties**.



Select **Port 1** and the **Advanced** tab once more. Enable **Always Grant Port Open Requests**; this allows RSLinx to always open the RealPort COM2 regardless of the actually availability of cellular access to the Digi Connect WAN RG or Digi Connect WAN VPN. Click **Network**.



On this final dialog screen, enable **Optimize for Cellular**. Click **Ok** on all dialog boxes to return to the Windows **Device Manager**.



When you return to Windows Device Manager, *it may appear to “hang”*. Just be patient, and in a few minutes, it will refresh its screen and can be closed. This delay occurs because RealPort needs to close the old cellular connection, reconfigure, and reopen the connection.

6 Running RSLinx 2.43.00

The example below assumes Digi RealPort has been configured to connect to the Digi Connect WAN RG or Digi Connect WAN VPN by COM2. If you had to use a different port number, then substitute that name into the examples below. The MicroLogix 1200 used in this example is configured for 19200 baud.

6.1 Adding a new RS-232 DF1 Device to RSLinx

Under **Communications > Configure Drivers**, add a new driver of type **RS-232 DF1 devices** and configure the fields as appropriate for the MicroLogix 1200. In this example the driver was renamed from AB_DF1-2 to AB_DF1-DIGI.



Configure RS-232 DF1 Devices

Device Name: AB_DF1-DIG

Comm Port: COM2 Device: SLC-CH0/Micro/PaneView

Baud Rate: 19200 Station Number: 00
(Decimal)

Parity: None Error Checking: CRC

Stop Bits: 1 Protocol: Full Duplex

Auto-Configure

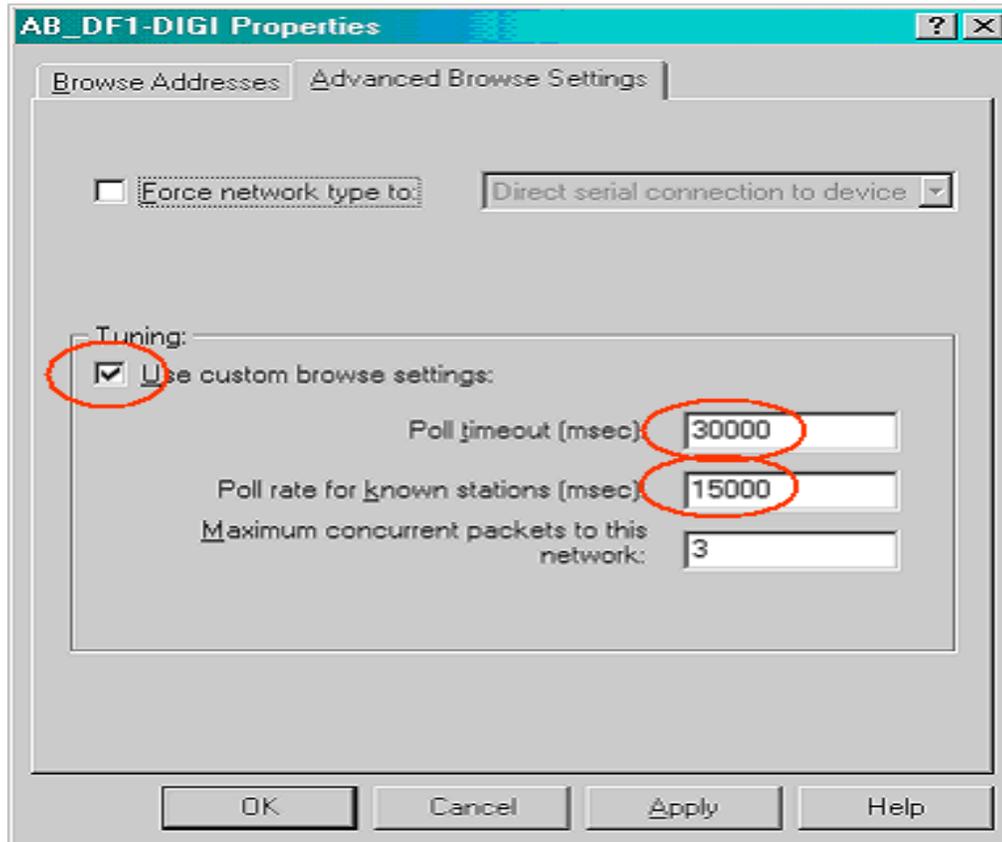
Use Modem Dialer Configure Dialer

OK Cancel Delete Help

Note that **Auto-Configure** can be used with Digi RealPort *only* if the Digi device is directly connected by Ethernet to your computer. **Auto-Configure** will not work for a device connected by cellular (wide-area-network), because RSLinx will not understand to wait long enough between various trial settings to properly detect valid responses.

6.2 Adjusting response timeouts

In the main RSWho window, right-click the AB_DF1-DIGI driver and select **Properties...** Enable the **Tuning** check box and change the **Poll timeout** to 30 or 60 seconds. Slow the **Poll rate for known stations** to a reasonable value, such as 15,000 msec (15 seconds).



6.3 Adjusting ACK timeouts

RSLinx does not understand that long responses such as 60 seconds imply a longer ACK timeout. As of RSLinx version 2.43, the ACK timeout is set based solely upon baud rate, with 9600 or 19200 baud forcing a 2 second ACK timeout. This is far too short an ACK timeout for a WAN connection – 20 or 30 seconds is a more appropriate ACK timeout. If you leave the ACK timeout at 2 seconds, RSLinx will send far too many ENQ.

Unfortunately, to adjust ACK timeouts, you need to edit the Windows registry. The key is:

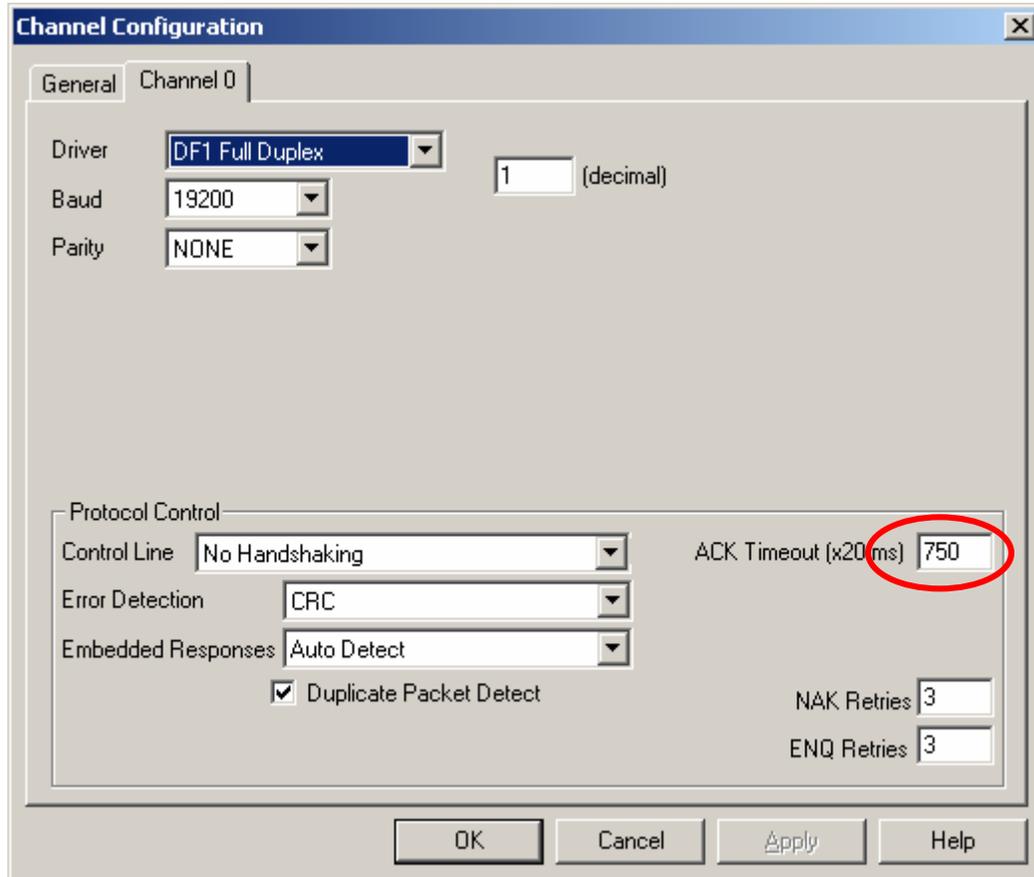
```
HKEY_LOCAL_MACHINE\SOFTWARE\Rockwell Software\RSLinx\Drivers\AB_DF1\AB_DF1-1
```

with the last name **AB_DF1-1** matching your driver as installed. The default value is 2000 – change this to 30000 if your response timeout is 60 seconds, and 20000 if your response timeout is 30 seconds. RSLinx will restore the old value if you change any of the DF1 settings. Then you will need to re-edit the registry.



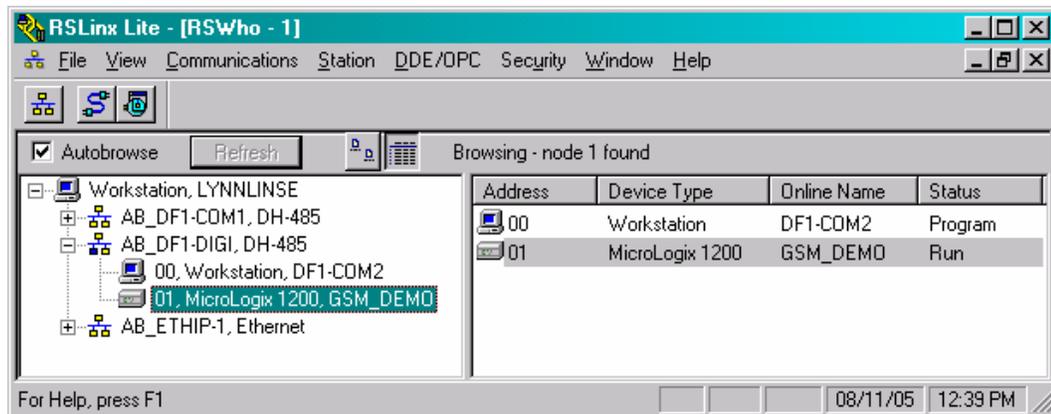
6.4 Changing ACK timeout in RSLogix 500

You must also change the DF1 driver of the PLC to understand the longer ACK timeout. Following is the Channel Configuration for a MicroLogix 1200. The new value of 750 sets a 15-second ACK timeout.



6.5 RSWho Results

If everything is set up correctly and no other user has connected to the Digi device and PLC, you will see the RSWho window such as this.





7 Removing RealPort

You do not want to leave RealPort active when you no longer desire access to the remote device. Because Digi RealPort will automatically attempt to connect to the Digi device every time you run Windows, it will impact your computer needlessly if left active.

7.1 Removing specific “adapters” from with Windows Device Manager

Right-click the device and select to **uninstall**. Windows asks you to confirm the uninstall, then removes the selected Digi device. In our example above this was called **Standard RealPort Device (166.213.136.17)**.

7.2 Removing all from the Command Prompt

Alternatively, you can run the original **Setup.exe** command line using the option **/removeall** to remove all Digi RealPort drivers installed.

```
Command Prompt
C:\Digi\rp_aug2005>dir
Volume in drive C has no label.
Volume Serial Number is 2450-7EE8

Directory of C:\Digi\rp_aug2005

11-08-05  03:24p        <DIR>          -
11-08-05  03:24p        <DIR>          -
19-07-05  04:35p           22,048  cocpyinf.dll
11-08-05  03:24p              0  CONERR$
19-07-05  04:40p          729,210  DgRpEncx.exe
19-07-05  04:35p           28,352  DgRpHelp.chm
19-07-05  04:40p          102,520  dgrpsetu.dll
19-07-05  04:40p          536,704  dgrpui36.dll
19-07-05  04:39p          108,922  DigiRIPt.sys
19-07-05  04:40p           3,907  digirp.inf
19-07-05  04:40p           3,617  digirprt.inf
19-07-05  04:35p            8,297  Readme.txt
19-07-05  04:41p           86,143  Setup.com
19-07-05  04:41p          573,569  Setup.exe
          12 File(s)      2,203,289 bytes
          2 Dir(s)    34,689,024,000 bytes free

C:\Digi\rp_aug2005>setup.exe /removeall_
```



8 Troubleshooting and FAQ

8.1 Can I access a MicroLogix 1000?

No – only a 1200 or 1500. The 1000 does not allow changing the ACK timeout.

8.2 Can I use DF1 Radio Modem Protocol?

Yes, as well as DF1 Full or Half-Duplex. The current firmware in the Digi Connect WAN family is not protocol-aware, and all bytes are passed through verbatim.

8.3 Can I bridge CSP or Ethernet/IP to serial DF1?

No – the current firmware in the Digi Connect WAN family is not protocol-aware, and is not attempting to bridge protocols. You can use a Digi One IAP or Rockwell 1761-NET-ENI after the Digi device to provide bridging.

8.4 Can I use RSLogix to upload/download?

Yes – However, RSLogix works in a half-duplex manner sending many small poll/response style packets. So the added end-to-end latency means it can take a long time to go online with a cellular-enabled PLC. For example, RSLogix5000 takes nearly 5 minutes to go online with a ControlLogix 1756-L55 processor. So you should not expect to do this routinely.

8.5 Why does the PLC keep going offline under RSLinx?

You must change the timeouts within RSLinx to be longer than default. Even with the changed timeouts, occasionally you will see the PLC offline or even as an "Unknown Device," since RSLinx only waits about 20 seconds for TCP sockets to open. Occasionally, when trying to connect, RSLinx will decide the remote PLC speaks neither CSP nor Ethernet/IP.

For serial PLC access, you must also edit the system registry for serial PLC access and change the ACK timeout setting within your PLC program.