MIRION TECHNOLOGIES

Application Note

Setting up a Quick Local Area Network for CRemote General Nuclear Industry Application

Introduction to the fundamentals of CRemote and a standalone LAN for Mirion Contamination Monitors

All of the Mirion personnel contamination monitors come with a standard Ethernet port and are setup to do networking "out of the box". This networking can provide easy access to the monitors via a central PC which enables Radiation Protection (RP) personnel to get the operational status of equipment, track and clear potential instrument faults, view the interior of the monitor via integrated video camera, communicate with personnel in the monitor via speaker and headset, obtain photographic data of personnel identity when a contamination event occurs and get instant pictorial displays of the contamination's magnitude and location.

This Application Note, the first in a series of contamination monitor specific network communication applications, will focus on the setup of a basic standalone network to enable communication between a dedicated PC and a series of contamination monitors to report instrument status, view fault conditions, and transmit radiation monitoring data from the contamination monitors to a PC located nearby the RCA exit. A few of the future Contamination Monitor Application Notes will cover the following topics:

- Setting up video monitoring and audio connections and communications between contamination monitors equipped with the IP Camera option (Argos™ and GEM™-5 series monitors).
- Capturing event driven digital photographic records on instruments with the IP Camera option.
- Configuring CRemote to remote control contamination monitors.
- Updating this application note for the use of Windows 7.
- Configuring and calibrating the AccuRate™ morphology and self-shielding parameters.
- Getting the most of the Self Shielding and Alarm Testing parameters on GEM-5 gamma exit monitors.

Background (problem)

Network Security at the majority of nuclear facilities has become so burdensome that the simple addition of a computer is time consuming and often so cumbersome in review and procedures that many RP organizations simply give up. Other barriers to establishing even a standalone network may include the lack of networking expertise, or just the time required to perform the setup. Our Application Support Group and experienced Field Support staff are available to assist in setting up network communications for these contamination monitors.

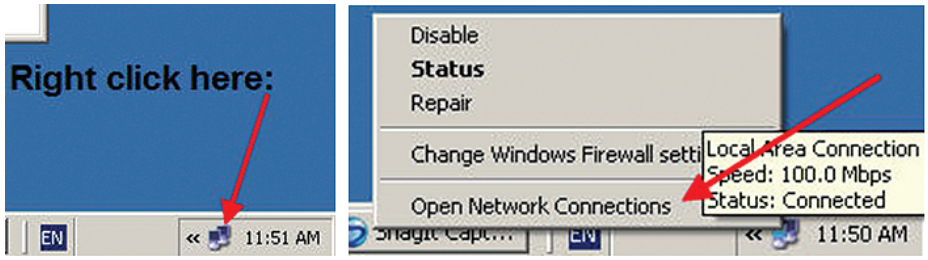
Equipment Needed

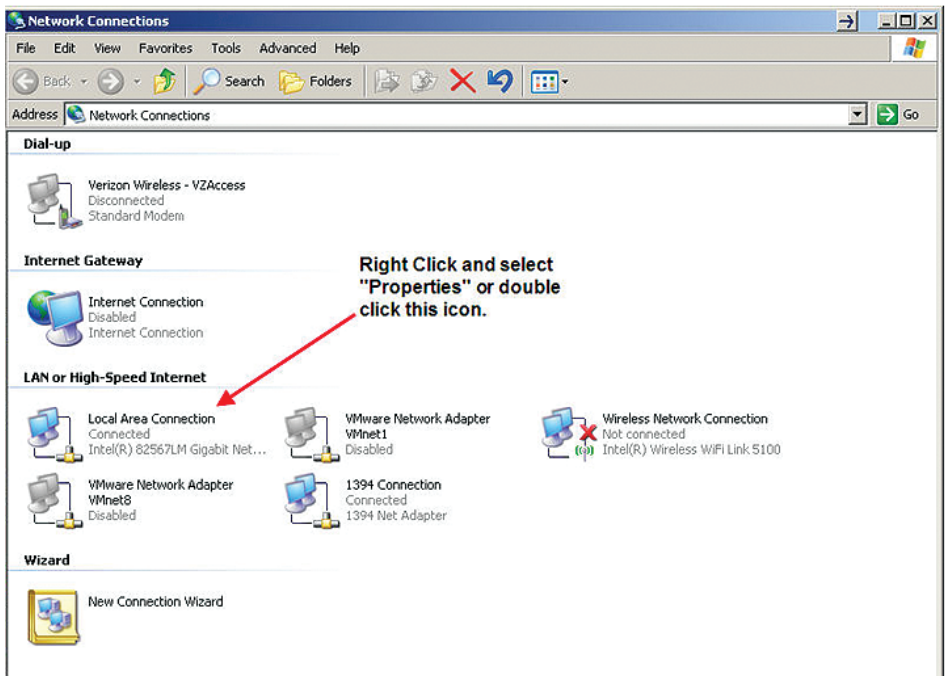
- Standard plenum rated CAT5e or 6E network cable-length to be determined by distance between the monitors and the standalone PC. Plenum rated cable is suggested as it meets specific ANSI/NFPA standards to be flame retardant and have low smoke production in a fire. Make sure your cable complies with this standard.
- RJ-45 Connectors and Network Cable Crimpers and wire strippers, cable ties. If you don't want to make your own cables, there are any number of companies who can make cables to your length specifications.
- Contamination Monitor(s): we will be using Monitor software Version 8.03 but this currently works up to monitor version 8.04.5.
- Wireless Network Router (wireless is optional).
- Network Switch(s) maybe optional depending upon the number of monitors and the distance between the RCA exit point and the RP office.
- CRemote Software (Version 1.06 will be used here).
- A standalone PC. Either a desktop or laptop will be sufficient. We'll set this up using an older spare/unused PC running Windows XP Professional. This Application Note will be updated shortly for using Windows 7.

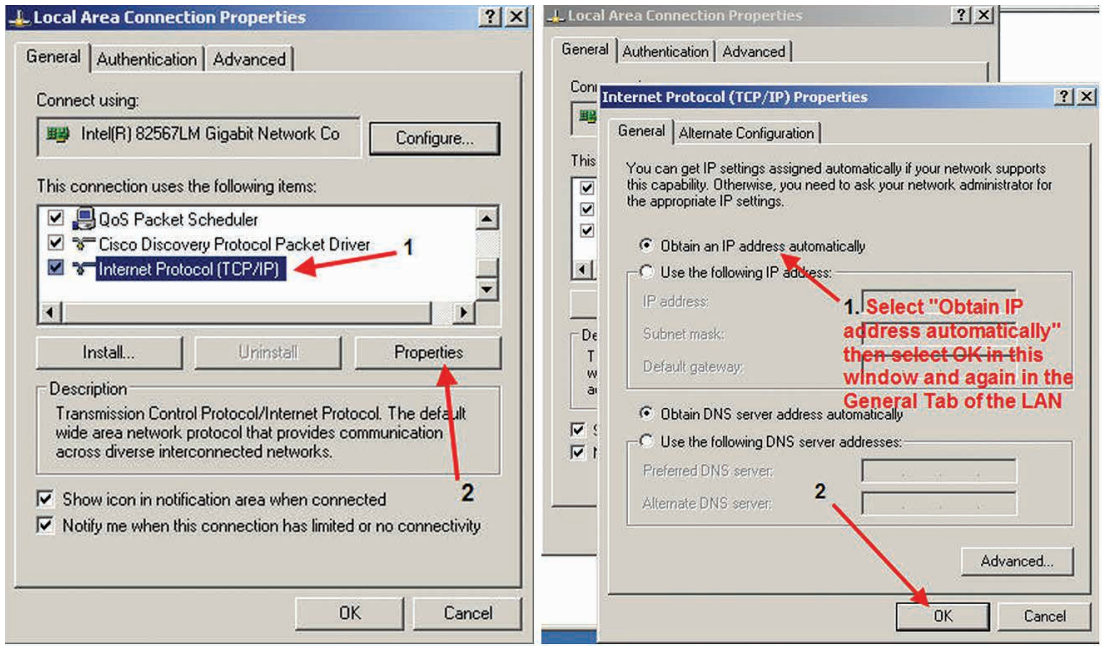
Basic Network Setup

We'll be setting up a simple network using a Netgear Wireless G Router model WGR614 v10. In order to configure your network, most (if not all) routers have an internal web server to configure the router. Netgear routers have all the default addresses and passwords on the bottom of the unit for beginning startup. We will use the default username and password in this example, although these may be changed in the router setup if needed. You will need to configure the router by connecting a network port of the Router with an Ethernet cable and run it to the network port of your PC. Plug in and power the router and your computer if it is not already on.

Configure your laptop for DHCP (Dynamic Host Control Protocol). This will enable the Router, once configured, to assign an IP address to your laptop. Open the control panel via Start→Programs→Control Panel and double click on the Network Connections icon, or right click on the network icon in the lower right corner of the main windows desktop. Follow the pictorials below:







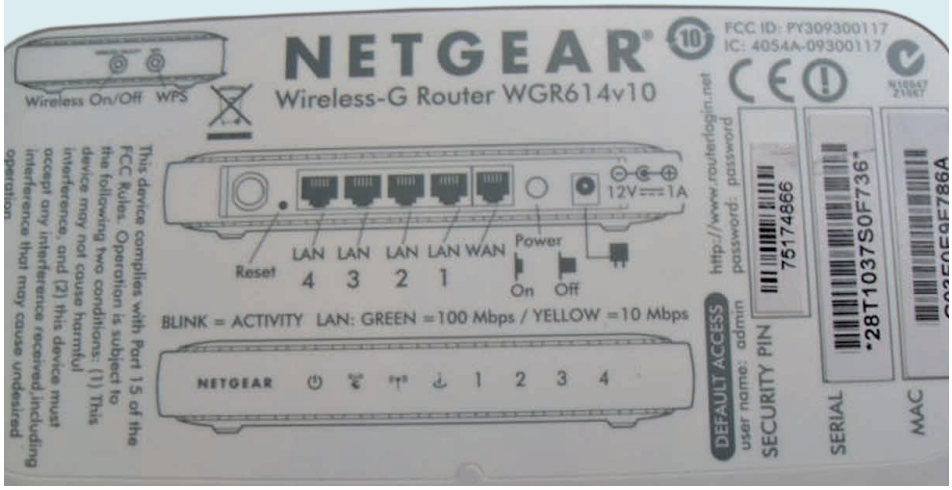
Now open a browser on your PC. Repeat this configuration step on all the monitors by escaping out of the program, exiting the monitor program by pressing CTRL-F4. Logout as the Monitor user, and Login as the Administrator to make these changes.

Once you have applied these changes, you will need to connect all the contamination monitors to a network switch (the size of the switch # of ports, will depend on the total number of contamination monitors you have. If you just have a few monitors and you have enough open ports on the back of your router, you can use your router by itself). You will need one LAN port to connect your PC to the Router, and the remaining open LAN ports will be used by your contamination monitors. If you have more monitors than you have available LAN ports, then you will need a Network Switch(s) to add more monitors. Connect any LAN port of your switch back to another switch, and ultimately one network cable needs to be connected to a LAN port of the Router to connect all the monitors, and switches to the same network. Do not use the WAN port of the Router in this configuration.

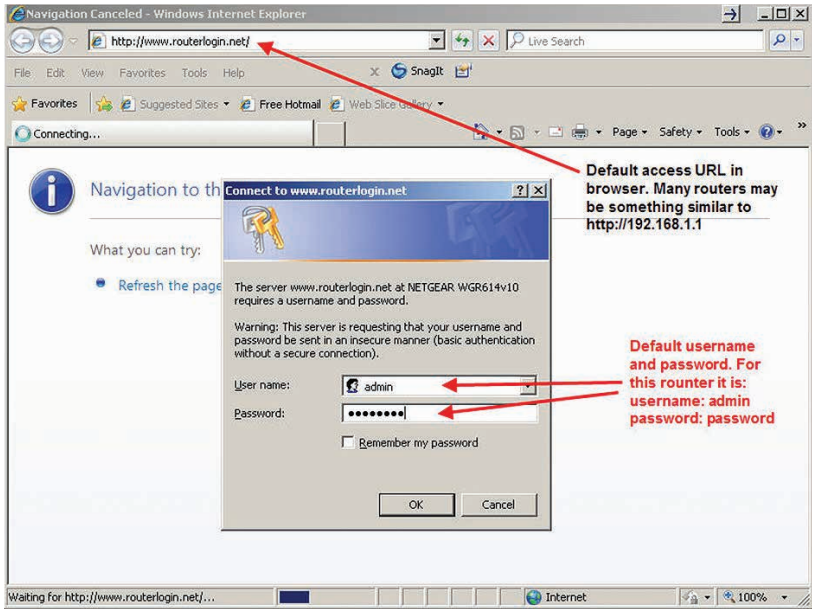
Configure your router

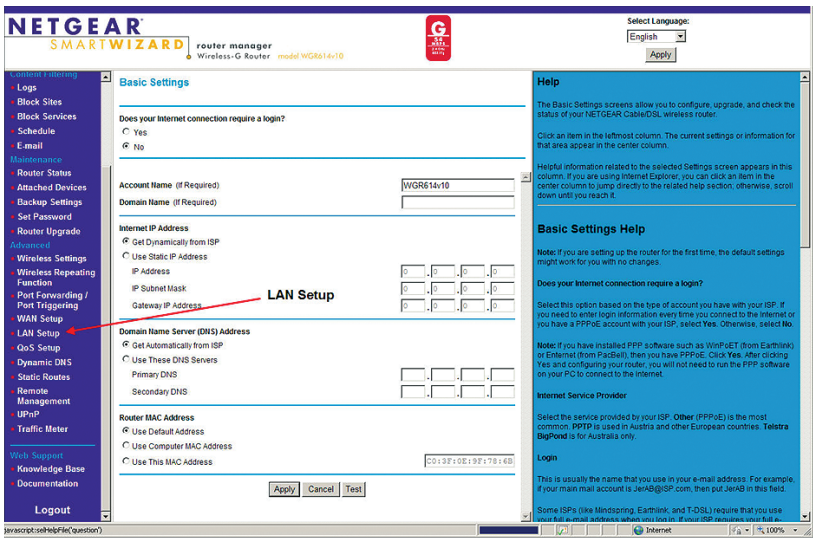
The basic router access default URL and username and passwords are usually listed on the bottom of the router, or in the user manual, in this case they are on the back of the router as seen below:

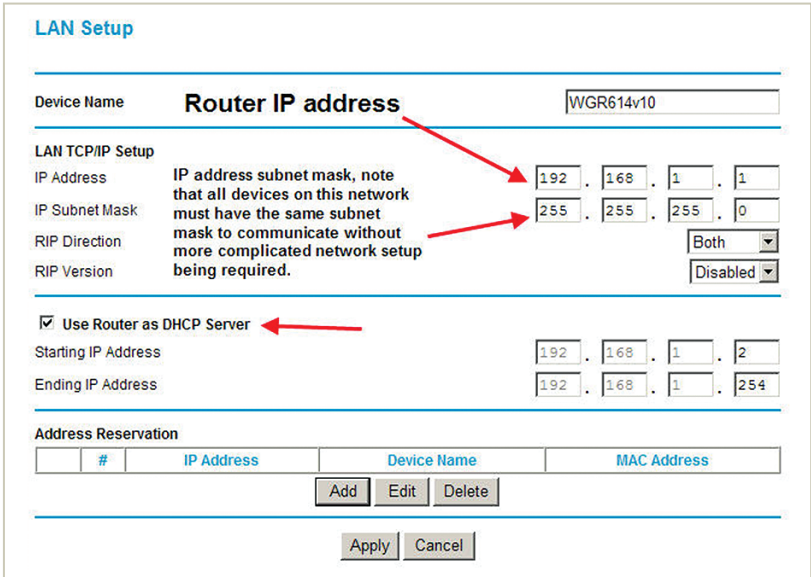
LAN and WAN port configuration of the Router



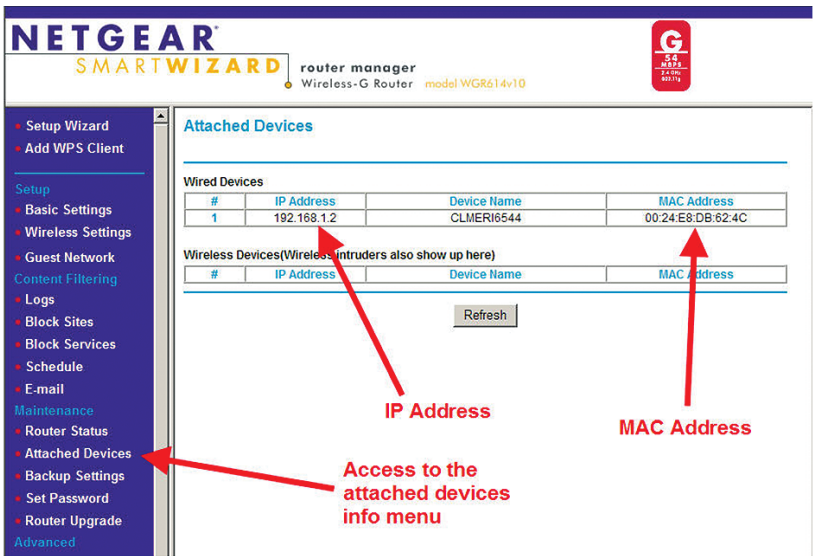
User name, password, URL


Navigation Canceled - Windows Internet Explorer
http://www.routerlogin.net/
Default access URL in browser. Many routers may be something similar to http://192.168.1.1
Connect to www.routerlogin.net
The server www.routerlogin.net at NETGEAR WGR614v10 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name: admin
Password:
Remember my password
OK
Cancel
Default username and password. For this rounter it is: username: admin password: password

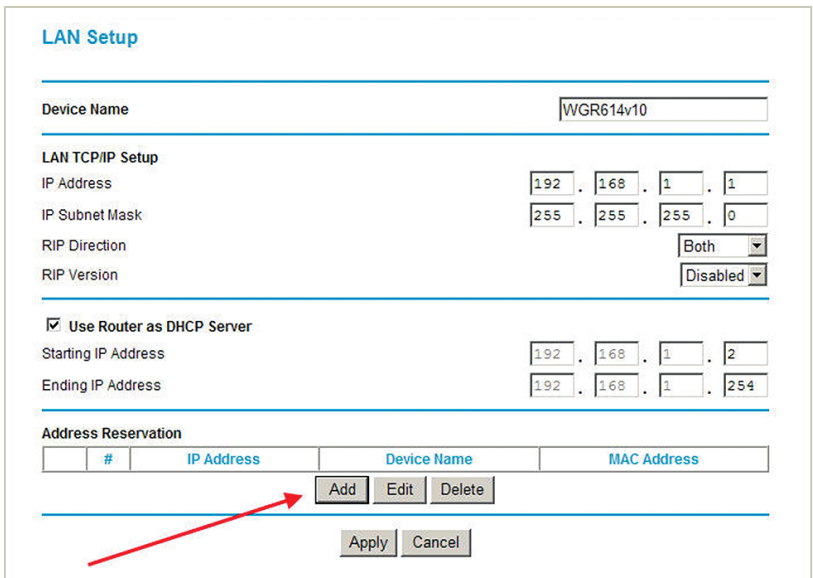

NETGEAR
SMARTWIZARD
router manager
Wireless-G Router
Basic Settings
LAN Setup
Help
Basic Settings Help


LAN Setup
Device Name
Router IP address
WGR614v10
LAN TCP/IP Setup
IP Address
IP Subnet Mask
RIP Direction
RIP Version
IP address subnet mask, note that all devices on this network must have the same subnet mask to communicate without more complicated network setup being required.
192 . 168 . 1 . 1
255 . 255 . 255 . 0
Both
Disabled
Use Router as DHCP Server
Starting IP Address
Ending IP Address
192 . 168 . 1 . 2
192 . 168 . 1 . 254
Address Reservation
IP Address Device Name MAC Address
Add Edit Delete
Apply Cancel

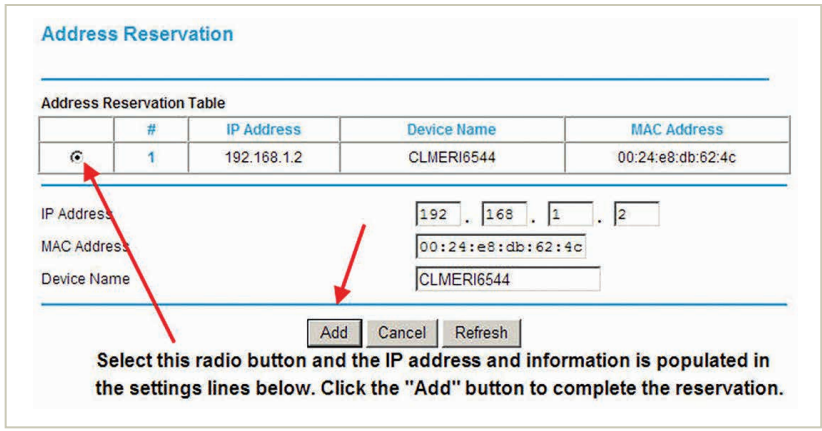
Select “Apply”. Network is now configured for DHCP and all devices connected to the network will now obtain an IP Address from your router. In order to keep everything constant, we will now add an IP Address Reservation for the PC running CRemote, as well as the IP Addresses of each monitor. Luckily the router has a utility menu which will collect all the device information that you will need in this case, the IP address of each monitor and the MAC Address of each monitor. This information is also populated in the LAN Setup screen when we select the “Add Reservation” button.



Select the LAN Setup on the left menu area which will take you to this screen. Then select the Add button.

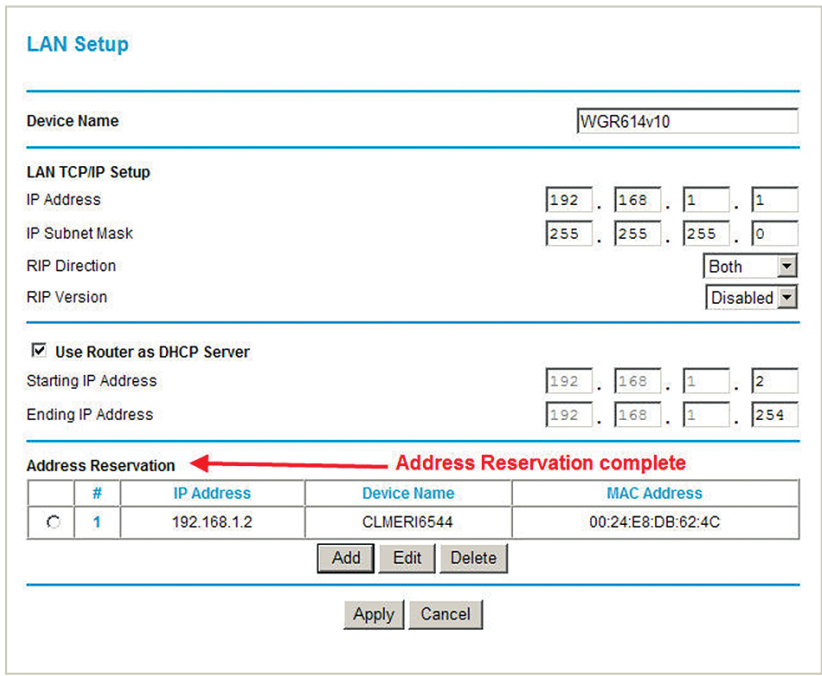


You will be taken to the Address Reservation Screen, Make your selections based on the following instructions:



Now the address reservation is complete for the PC to run CRemote. You will now need to connect cabling up from each contamination monitor and run the cable to the back of your router, or switch. A cable must be run from each contamination monitor to the router, or if you have multiple contamination monitors you may need to add switches.

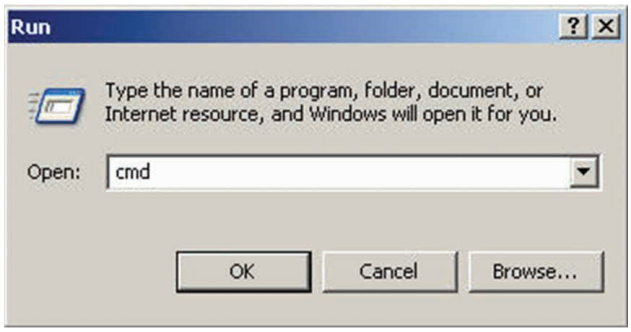
Repeat this for the remaining Monitors that are on the network. If they are all successfully connected, each monitor will appear in the menu above and can be selected and added.



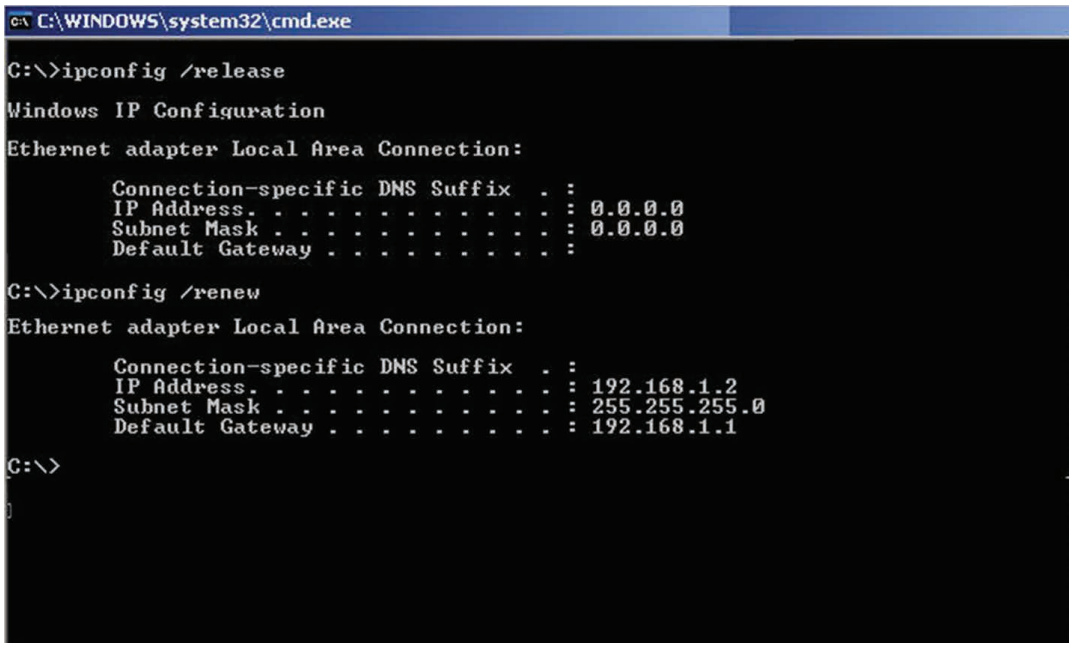
If a monitor is not available, the simplest way to add them is to restart each computer. To do this exit out of the Monitor program. ESC, then ALT-F4. Select Start→Shutdown→Restart the monitor. Upon restart the monitor should pickup the IP address from the Router.

Alternatively, one can also open up a command prompt window and use the ipconfig command as follows:

Start→run, then type “cmd” in the window, and hit the return key, or click on the OK button:

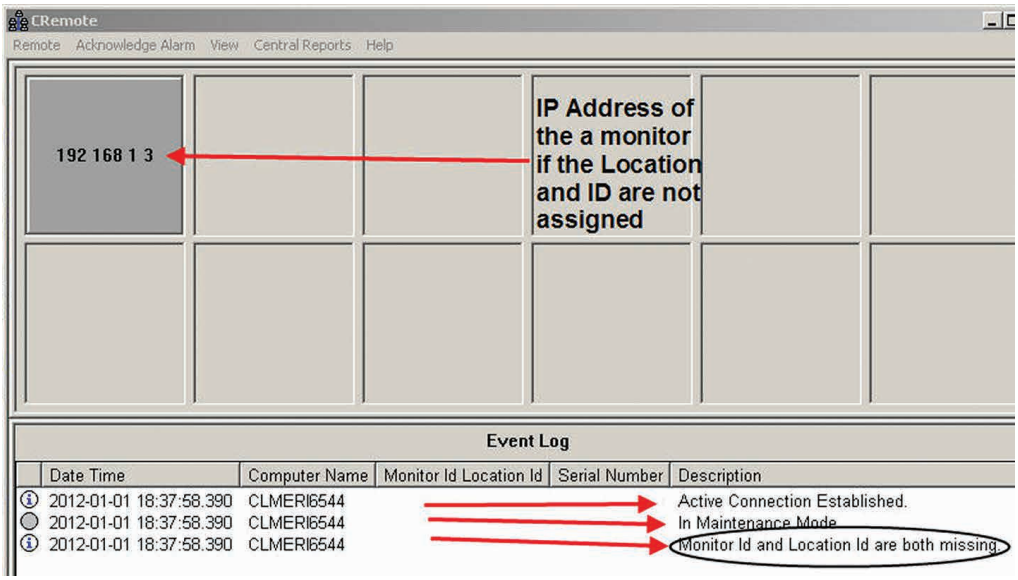


Then type the following commands in the command prompt window as seen below. This will release the IP, and then renew it with the reserved IP from the router.



At the completion of all these tasks, each monitor will now have an IP Address Reservation and be on the network. In the case here we see that the IP Address of the CRemote computer will be **192.168.1.2**. Save this IP address, you will need to enter it on each contamination monitor when configuring the network parameters on each Contamination Monitor. For now install CRemote on the PC which will be the main "surveillance" PC at the RP satellite station for that RCA. Instructions for CRemote. Run the installer, when the installer is compete a CRemote short cut icon will be installed on the computer Desktop. Double click on the icon to launch the program.

The CRemote program will start up and appear somewhat like the figure below if the monitors are properly configured (we'll do this in a minute). If the Monitor ID and Location are not assigned in the Common Values Screen (Setup Menu→F1) CRemote will use the IP Address of the computer in that Monitor. Note that it is VERY important to pick the location and ID of the contamination monitor which is meaningful to your RP staff. Obviously, just an IP address is not very helpful.



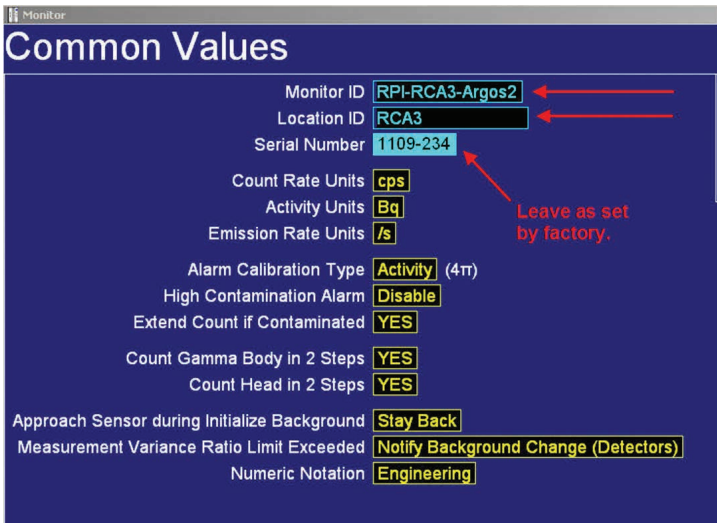
Monitor Program Software Setup

We'll be using an ARGOS-5AB system with the Zeus™ Gamma option as the example contamination monitor. However, the basic network settings and data communications will be identical for all our contamination monitors.

Let's look at the Setup required on the Argos monitor and see what's needed:

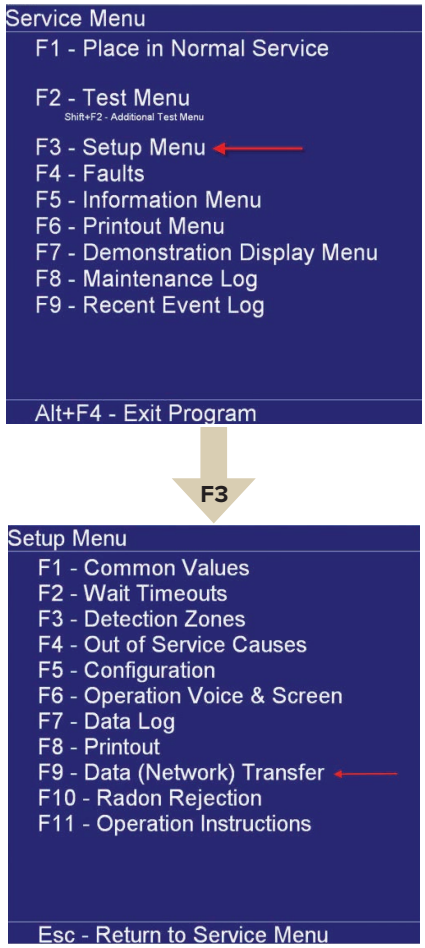
Common Values:

As we just mentioned, the screen below should have location and identification values which are meaningful. The values should enable your RP staff to easily identify the location of the monitors (such as RCA 3) and the ID of the monitor (perhaps a plant instrument code such as RPI-RCA-3-Argos2 (The Monitor ID and Location ID fields are currently limited to 15 characters). The Serial Number is the number assigned by the factory and should remain as it was assigned. This enables ease of diagnostics by Mirion if DATALOG files are sent to Service. The format of the serial number is YYMM-XXX (year and month of manufacture, and the number of the monitor produced that year in sequential order).

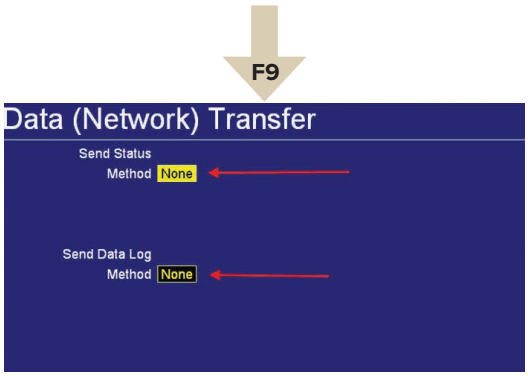


Networking:

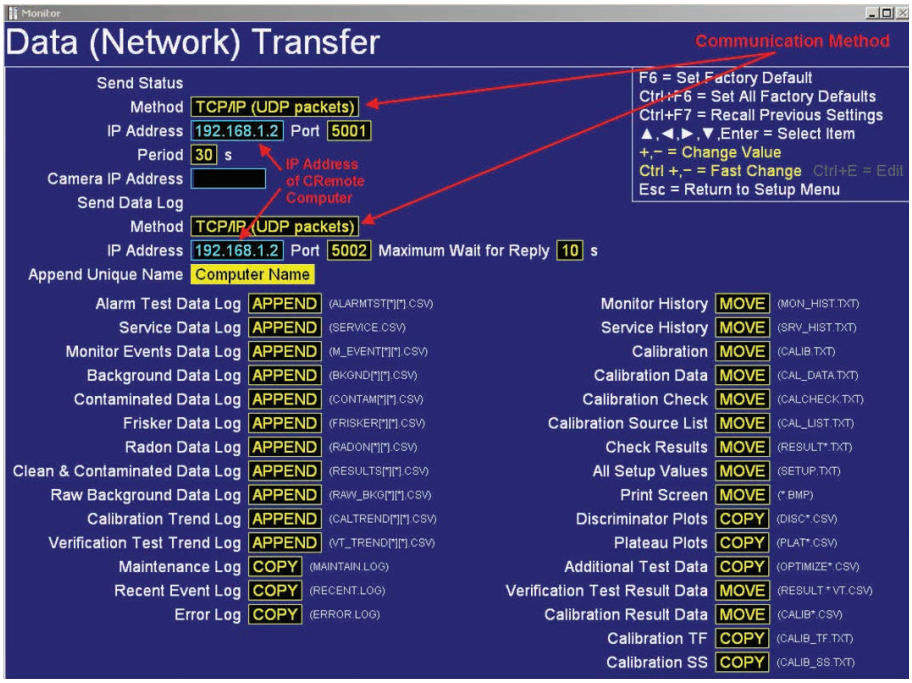
Get to the Service Menu of the monitor (available by using the USB keyboard plugged into the computer of the monitor) by pressing the escape key. Once in the Service Menu, press the F3 key for the Setup Menu and then F9 the Data (Network) Transfer Screen.



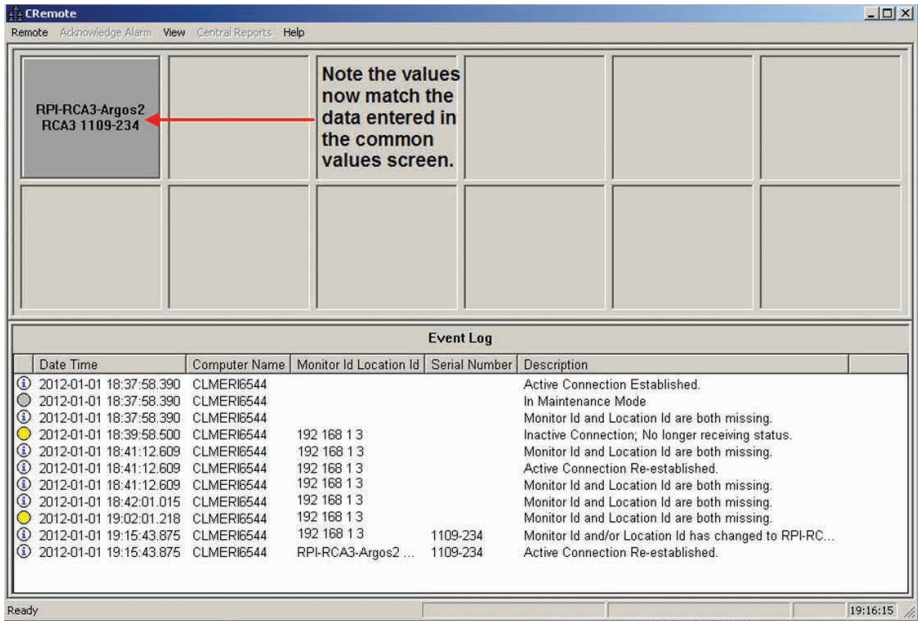
Using the keyboard toggle the ± key on the Send Status Screen to set this to “YES”. Press the “ESC” key twice to retain your settings and return to the Service Menu. (Note that your menu may appear different for other settings, as these screen captures have been produced on a demonstration software version of the monitor.)



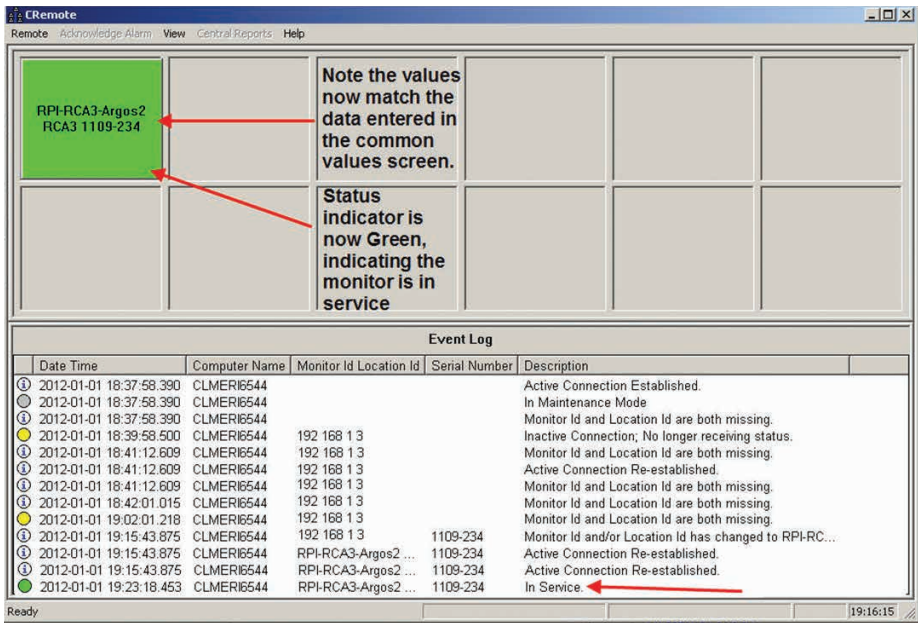
Using the keyboard toggle the ± key on the Send Status Screen to set this to “YES”. Press the “ESC” key twice to retain your settings and return to the Service Menu. (Note that your menu may appear different for other settings, as these screen captures have been produced on a demonstration software version of the monitor.)



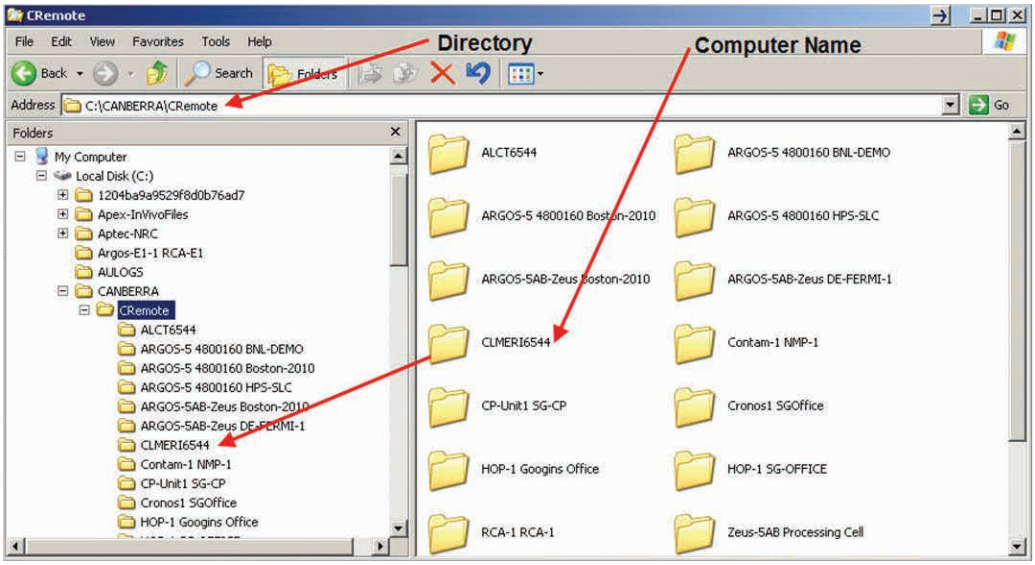
Once the values are set, escape back to the Service Menu. The CRemote Screen should now look like this (obviously your Common Values information will differ from this example).



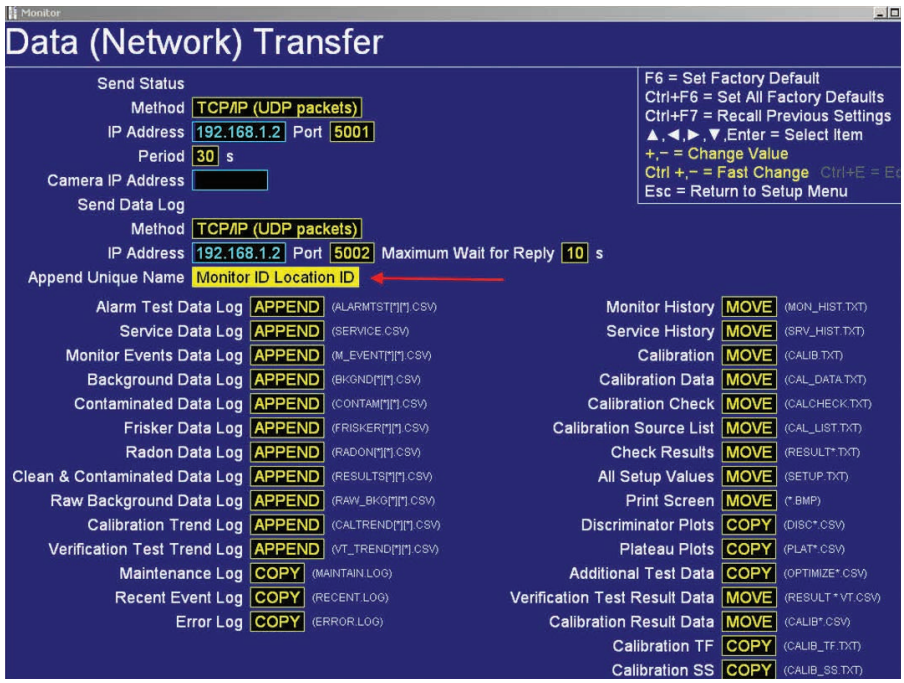
Now place the monitor into service and the CRemote Console will appear as follows (the green status block indicates that the monitor has entered normal service):



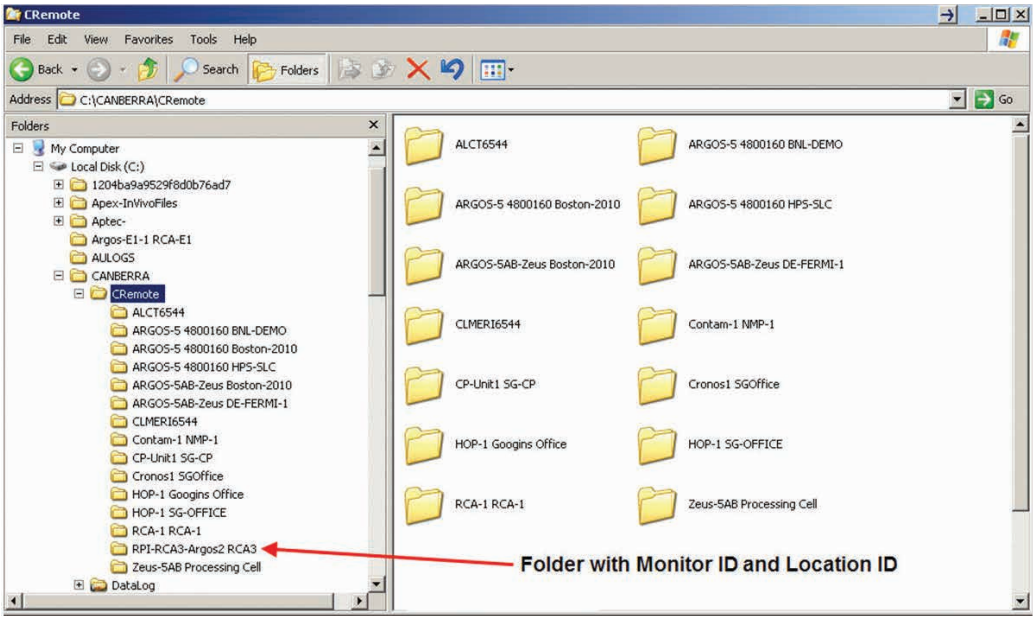
What has also happened on the computer running CRemote is that individual folders for each monitor have been added in the CRemote Program folder which contain all the data from the monitor (at the present time we have the folder appended with the Computer Name of the Monitor):



If we change the setup in the Data (Network) Transfer folder to “Monitor ID Location ID” this unique name will now be the folder name with all the data:



And now the director structure has added the folder with this unique information which is much more useful:



Now CRemote has been setup on a standalone network with a PC and some networking gear. If you have questions, don't hesitate to contact the Application Support Group through our main customer service number. Application Support Managers or Field Service Engineers can also help you setup a standalone network as part of a service contact or service agreement.

References

1. Institute of Nuclear Power Operations *(INPO) INPO 05-008 Guidelines for Radiological Protection at Nuclear Power Stations* (2005).
2. American Nuclear Insurers (ANI) *ANI Section 8.5 Radiation Protection Bioassay*. (2008).
3. Argos-3/-5 Whole Body Surface Contamination Monitors, User's Manual, Canberra Industries (2010).

www.mirion.com

Copyright ©2018 Mirion Technologies, Inc. or its affiliates. All rights reserved. Mirion, the Mirion logo, Canberra, Argos, GEM, AccuRate, Zeus and other trade names of Mirion products listed herein are trademarks and/or registered trademarks of Mirion Technologies, Inc. and/or its affiliates in the United States and/or other countries.

Third party trademarks mentioned are the property of their respective owners.

C39337 - 11/2012